THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 11 NUMBER 2
AND HOMELAND SECURITY

AUGUST 2012
SMART-GRID SECURITY

Contact: dhardy1@gmu.edu
703.993.8591

Click here to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

In this month's issue of *The CIP Report*, we highlight the significance of and the challenges with securing the smart grid. The critical role of the smart grid was recently displayed in India, when more than half of its population lost power due to the failure of its energy infrastructure, and in Virginia, where power companies and residents were unprepared for the consequences of an unexpected, violent "derecho" storm. To further complicate the matter, the various companies and governments responsible for protecting this critical infrastructure are challenged by its interdependencies with other sectors, including cybersecurity and supply chain security, which introduces new stakeholders into the legislative and security fray.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, the Deputy Assistant Secretary for Research and Development (R&D), Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy provides an overview of smart grid security. The findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience, which include best practices in supply chain security and resilience that help to reduce cyber risks, are revealed. Then, Progress Energy explains their collaborative efforts in building bridges between operations technology (OT), information technology (IT), and supply chain professionals and Schweitzer Engineering Laboratory (SEL) analyzes their best practices designed to ensure supply chain security in smart grid components. Next, in a collection of vignettes, different companies illustrate their best practices in supply chain security, resilience, and integrity. Finally, the Director of Global Supply Chain Security with the National Security Staff describes the U.S. government's integrated and collaborative approach to enhancing global supply chain security.

This month's *Legal Insights* examines the legislative obstacles that confront the numerous domestic and international governments and industries responsible for protecting the smart grid.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Securing the Smart Grid: Roadmap for the Future

by Hank Kenchington,
Deputy Assistant Secretary R&D, Office of Electricity Delivery and Energy Reliability,
Department of Energy

The integration of intelligent technologies throughout the power grid can revolutionize our economy, provided that we can adapt to a changing risk landscape and effectively harness the expertise, knowledge, and resources of private- and public-sector partners.

A Smarter Grid Can Power a Cleaner, High-Growth Economy

The integration of information and communications technologies throughout the power grid is revolutionizing the way electricity is delivered and used. Intelligent systems and two-way communications are bringing a host of advancements to the grid — from time-of-use pricing and smart metering to faster outage detection and service restoration. These technologies will enable the sector to:

- ***Monitor and manage the power system in real-time, creating both greater energy efficiency and operational resilience:*** New information flows give utility operators more visibility into the real-time behavior of the grid. Millions of digital devices interconnected through modern communications networks will collect data to better understand the behavior of the grid, enable greater automation to reduce outages, and improve system efficiency.

- ***Provide information that will enable customers to better manage electricity usage:*** The smart grid uses two-way communications to allow utilities, customers, and even third-party service providers to actively participate in energy markets. For example, dynamic price signals sent to customers' smart meters will allow them to align their usage with price incentives. New smart devices and appliances can respond to pricing signals and turn off when power is most expensive and back on when power is cheaper. This also helps utilities hold down costs by reducing the use of inefficient peak generation equipment and deferring construction of additional generation capacity.

- ***Integrate renewable sources of energy:*** The smart grid helps the shift to a clean energy economy by better integrating distributed and variable generation sources such as wind or solar. Since the availability of wind and solar resources does not always match up with consumer demand, utilities can use smart grid technology to more quickly recognize changes in electric power supply and implement actions to maintain system reliability.

Most importantly, the smart grid will power America's competitiveness in the 21st century.

The Benefits of the Smart Grid are Accompanied by New Cybersecurity Challenges

Increasing the use of information, communications, and control technologies can make electricity delivery more reliable. For example, new sensing and control systems are able to detect disturbances and re-route power in real-time to avoid outages. This feature and a host of others help reduce the risk of outage from storms and other natural events.

These same systems create new risks. In the past, the communications networks used by utilities to control grid operations were largely isolated from other networks, making them relatively less susceptible to cyber-attacks. Interconnected digital communications used in today's networks and the growing use of common protocols — a core building block of the smart grid — can create conduits for attacks against the power system. The cyber threat landscape is dynamic — changing as rapidly as the new technologies and capabilities

(Continued on Page 3)

Smart Grid Security *(Cont. from 2)*

designed to thwart attacks.

The U.S. Department of Energy (DOE) has a long history of working closely with industry and Federal partners, including the U.S. Department of Homeland Security (DHS), National Institute of Standards and Technology (NIST), and the U.S. Department of Defense, and other stakeholders to enhance the cybersecurity of the grid. The nascent nature of the smart grid provides a great opportunity to "build in" security from the onset — when it is most cost effective.

Our work with the electricity sector has highlighted some basic principles for the cybersecurity bottom line:

- ***Cybersecurity is vital, but there is no 100% solution***: No matter how deep our defenses, we have to plan for the reality that it may not be possible to intercept every attack. So, we have to work together to engineer a system that has survivability. As laid out in the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, we need systems that can survive a cyber incident and maintain critical functions even under attack.

- ***Not all devices are created equal***: With potentially millions of devices on the system, it is not feasible or affordable to give every component the same level of security and protection. We need a risk-based framework, based on potential impact, to guide resource allocation and attention at the national level.

- ***Neither the government nor the private sector can go it alone:*** The White House expressed it well in their *2011 Policy Framework for the 21st Century Grid*: "facilitating a smarter and more secure grid will require sustained cooperation among the private sector, state and local governments, the Federal government, consumer groups and other stakeholders."[1]

Reducing Risk Through Public-Private Partnerships

Public-private partnerships are crucial to address complex challenges like cybersecurity. When effectively managed, collaborative partnerships become powerful tools. But, public-private partnerships sometimes tend to be top-down, rather than two-way. We need to get down to the business of creating partnerships that deliver results.

What makes an effective partnership? At the core is a willingness to align resources to achieve a common outcome that benefits all partners, even if the partners are motivated by different objectives.

While there is no perfect model for success, there are three basic ingredients:

1) **Create a Common Vision and a Roadmap to Get There**: Can we agree on what the end state is? Can we jointly create a pathway to achieving that end state, with defined benefits for all sides?

2) **Commit to the Actions Needed to Implement the Roadmap**: Can we clarify the roles and responsibilities of partners to leverage their greatest strength?

3) **Measure Progress**: Are we delivering results and achieving the desired outcomes?

For partnerships to work, the parties need to commit resources and the benefits of collaboration need to outweigh the costs. In our partnership with energy companies, industry took the lead in defining a vision and identifying priorities in the roadmap. This was with good reason: the private sector has the biggest task of building and securing the sophisticated communications networks, digital components, and other facilities that will form a smart grid while reliably operating a complex and dynamic electrical system.

Government has an important role too. Today's cyber risks extend beyond organizational and geographic boundaries, exposing utilities to threats they have never faced before. We expect utilities to be able to deal with many types of risks, but we cannot expect them to secure their networks against targeted, international cyber threats. Government needs to develop the advanced tools, global awareness, and strategies to help defend critical infrastructure against sophisticated

(Continued on Page 4)

[1] The White House, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future,* (June 2011), http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

Smart Grid Security *(Cont. from 3)*

cyber threats. We also need to improve how we share information — in both directions. Lastly, we need to be able to do this at network speed.

Collaborative efforts to secure the smart grid have been gaining momentum since DOE created a full-scale test bed for supervisory control and data acquisition (SCADA) systems in 2003. Each initiative — from the creation of a National SCADA Test Bed, to the development of a consensus roadmap, to the recently released *Electric Subsector Cybersecurity Capability Maturity Model* — has further strengthened the trusted relationship between government and industry and enhanced the effectiveness of the collaboration. Each step in the process created greater clarity about roles and responsibilities; shared knowledge about capabilities and best practices; and helped build trust.

National SCADA Test Bed

As concerns about new cybersecurity threats began to rise in the early 2000s, one obstacle to addressing those risks was the lack of tools to test the security of the SCADA systems used to manage and monitor large portions of the grid. In 2003, DOE created the National SCADA Test Bed at the Idaho National Laboratory (INL) and ultimately expanded it across the Department's laboratory system to create a national resource to support control systems security in the energy sector. Agreements were forged with major vendors of control system equipment to test their system on a realistic, but safe network. Cybersecurity experts used the latest cyber-attack tools to identify control system weaknesses. An assessment was provided to each vendor — with follow-up testing to evaluate the effectiveness of the mitigations. Vendors then shared this information with their utility customers through user group meetings.

Greater confidence in the tested systems created market demand — major utilities now insist that new SCADA purchases are tested for security vulnerabilities. As a result, most large SCADA systems offered today for energy management applications have been tested and improved to enhance cybersecurity.

Roadmap to Secure Control Systems in the Energy Sector

Independent SCADA testing was a good first step but it represented just one solution to a complex problem. We needed a larger framework to identify all the challenges and approaches to improve control system security. In 2005, government and industry came together to create a common vision and agenda for cybersecurity. With the realization that 100% security was not an achievable objective, the partners addressed the need to define an end goal: to survive a cyber assault with no loss of critical function.

The *Roadmap* was built on the collective insights of asset owners and operators, commercial vendors, national laboratories, academia, industry associations, and government agencies. Arguably, the first critical infrastructure resilience effort, it provided a common vision and collective plan to improve cybersecurity through systems assessment, next-generation R&D, best practices, and outreach. Indeed, the collaborative approach was so successful that it was subsequently replicated in the water, chemical, and nuclear sectors.

The *Roadmap* was updated in 2011 to address the expansion of smart grid technologies, evolving capabilities of the threat, and to take stock of what had been accomplished. For example, the *Roadmap* identified a need to protect SCADA communications between remote grid sensors and control centers. DOE's Pacific Northwest National Laboratory developed an innovative secure protocol that verifies that messages came from a trusted source and were not altered in transit. More importantly, the technique did not hamper delivery of time-critical data. The approach was field tested at CenterPoint Energy and the test findings reviewed by an advisory board of energy-sector industry experts. Schweitzer Engineering Laboratories (SEL) participated in the project and commercialized the first device. Bottom line: the first lot was sold out in short order and the devices are being deployed today to better secure the power grid.

Roadmap participants also identified the need for companies to be able to evaluate the functionality, performance, and interoperability

(Continued on Page 5)

Smart Grid Security *(Cont. from 4)*

of security products from different vendors before purchase. DOE's Sandia National Laboratories developed a framework to build security and interoperability into products made by different vendors. Using this framework, Sandia partnered with EnerNex Corporation, SEL, the Tennessee Valley Authority, and the Electric Power Research Institute to identify security features needed by industry, develop solutions that address these features in an easy-to-use way, and validate both their interoperability and reliability. As a result, SEL commercialized a gateway that secures routable communications across electronic security perimeters. Now more than 10 power grid security device vendors (such as GarrettCom, N-Dimension, and Industrial Defender) are using the results of this work to build security and interoperability into their smart grid devices. More importantly, these devices are being deployed today to enhance cybersecurity in the grid.

The *Roadmap* provides a framework for guiding both public and private actions to enhance cybersecurity. Since the original *Roadmap* was launched in 2006, many organizations have contributed. For example, DHS established the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to monitor and share information on emerging threats and vulnerabilities. NIST created the Smart Grid Interoperability Panel and developed *Guidelines for Smart Grid Cyber Security*. Led by the North American Electric Reliability Corporation (NERC), the electricity sector developed cybersecurity standards for the bulk power system and has been implementing and improving these standards since 2007. A more comprehensive list of contributors can be found in the 2011 Roadmap to *Achieve Energy Delivery Systems Cybersecurity*.

2012 Electricity Subsector Cybersecurity Risk Management Process Guideline:

The electricity subsector cybersecurity risk management process guideline was developed by a team of government and industry executives to enable organizations — irrespective of size or governance structure — to manage cyber risks at three levels within the organization:

- Executive Leadership: Executive level risk management with appropriate leadership involvement, management strategies, and resources;

- Business Management: Implement cybersecurity risk management goals and strategies into business processes; and

- Systems Management: Cybersecurity safeguards, controls, and countermeasures at the system level.

2012 Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The maturity model was designed to provide a common way for the industry to evaluate and benchmark cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity and share knowledge and best practices. The model includes 10 domains that each provide a structured set of cybersecurity practices designed to help utilities prioritize actions and investments that will improve cybersecurity. Numerous government, industry, and academic organizations participated in the development of the model, which was piloted at 17 utilities to validate the usefulness of the criteria and set of practices.

New Directions: Workshop on Best Practices in Supply Chain Security, Integrity, and Resilience to Secure the Smart Grid

The *Roadmap* goals have become effective rallying points for collaborative smart grid efforts —in new technology development, risk management processes, and a maturity model — and most recently to address smart grid supply chain risks.

One of the key "takeaways" is that although we have made great progress, there is no room for complacency. Rapid changes in technology, information, and infrastructure will continue to change both the threat potential and industry's risk profile. Supply chain is one of these new areas of concern.

The Workshop on Supply Chain Cybersecurity grew out of the realization that as we succeed in

(Continued on Page 26)

"Aha" Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience

by Debra van Opstal, U.S. Resilience Project

In March 2012, the U.S. Resilience Project organized a Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity and Resilience. Sponsored by DOE and George Mason University, the workshop engaged five partner organizations — the Edison Electric Institute, EnergySec, Gridwise Alliance, Internet Security Alliance, and the Supply Chain Risk Leadership Council — each of which brought experts and expertise to the dialogue. More than 90 participants representing different specialties and sectors — including the power industry, software, telecommunications, chemical, defense industrial base, aerospace, heavy manufacturing sectors, government, and academia — discussed how business best practices in supply chain could help reduce cyber risks to the smart grid.

The potential cyber vulnerabilities of the smart grid have dominated attention in both the public and private sectors. What makes the new grid "smart" are the interconnections that enable communications between devices, which in turn make the system more agile, adaptive, and able to preempt disturbances. But, embedded IT devices throughout the system also create more access points for potential disruption. A few examples of IT vulnerabilities:

- In August 2003, the "Slammer" worm infected the Davis Besse nuclear power plant in Ohio, causing a five-hour shutdown of computer systems.

- In October 2006, a foreign hacker invaded the Harrisburg, PA, water filtration system and planted malware.

- In June 2008, the Hatch nuke plant in Georgia shut down for two days after an engineer loaded a software update for a business network that also rebooted the plant's power control system.

- In April 2009, T*he Wall Street Journal* reported that cyber spies had infiltrated the U.S. electric grid and left behind software that could be used to disrupt the system. The hackers came from China, Russia, and other nations and were on a fishing expedition to map out the system.

- Discovered in June 2010, the Stuxnet computer worm attacked specific industrial control systems, mostly in Iran, where they were used to enrich uranium.

- The Flame virus, discovered in 2012, exploited the Windows operating system to capture audio, screenshots, keyboard activity, and network traffic information from infected computers. Flame is thought to have circulated on the Web for at least four years apparently without detection — and highlights some of the potential dangers of undetected malware.

To date, efforts to secure the smart grid have centered on threats that come across the information and communications networks. But, cybersecurity requires more than IT solutions. As IT systems and software become more secure, new threats to the smart grid are increasingly likely to come through the supply chains.

The Workshop focused on capturing industry best practices in the supply chain that could help prevent corrupted, counterfeit, or compromised components from entering the smart grid and identifying gaps and opportunities for public-private partnerships.

The discussion yielded 5 "aha" insights:

- Best practices in supply chain security and resilience already help to reduce cyber risks to the smart grid.

- A compelling business case can be made to support investment in smart grid supply chain security.

- There are synergies of solution in supply chain security, integrity, and resilience.

(Continued on Page 7)

Workshop *(Cont. from 6)*

• End-to-end organizational and operational approaches are needed to capitalize on synergies of solution.

• Government and industry objectives are more aligned than they sometimes appear.

1. Best Practices in Supply Chain Security and Resilience Help Reduce Cyber Risks to the Smart Grid

Supply chain practices have changed dramatically over the past 10 years — a decade that saw the emergence of global supply chains and increased disruption risks.

The multinationals of the 20th century typically cloned themselves, transplanting their operations as self-contained businesses to foreign shores so the impact of disruptions — whether accidental or deliberate — remained largely localized. But, the IT revolution of the late 1990s enabled the emergence of global enterprises — companies which spliced their operations across different geographies and networked them back together through global supply chains. While cost-effective, globalization amplified supply chain vulnerabilities; disruptions in one place or component have repercussions across the entire supply chain network. Extreme weather, geo-political turbulence, and black swans (Icelandic volcano and Japanese earthquake and reactor disaster) increased disruption risks while outsourcing increased the risks of counterfeit products, IP theft, and quality control problems.

Global enterprises managed these new risks by investing in more rigorous supply chain practices and controls — for security as well as resilience — and, in the process, developing some of the most sophisticated supply chain risk management processes and tools in the world. According to executives at Cisco, supply chain risk management practices moved from being reactive (responding to crises) to proactive (preparing for crises) to innovative (creating new tools that enable transparency, agility, and adaptability through the supply chain networks).

The smart grid has accelerated the globalization of the supply chain for utilities and reliance on foreign sources of supply. Cutting-edge practices, processes, and tools developed over the course of the last decade by the first wave of global enterprises can provide a benchmark of best practices for the smart grid industry and have the potential to reduce the risk of Trojan Horses in the smart grid supply chains.

2. There is a Compelling Business Case for Companies to Invest in Supply Chain Risk Management

Getting businesses to adopt supply chain best practices may not be a wild stretch, even in an age of cost-cutting. Supply chain has grown from a back office problem to a bet-the-company risk. Research on supply chain resilience by Singhal and Hendricks demonstrated that, of the 835 companies that announced a supply chain disruption between 1989 and 2000, 33-40 percent experienced lower stock returns than their industry peers, regardless of industry, cause of disruption, or time period. Changes in operating income, sales, total costs, and inventories remained negative in the two years after the problems were disclosed.[1]

According to a Dow case study, where investments in supply chain security were made, the company gained:

• More than 20 percent savings from reductions in excess inventory and container fleet requirements;
• 100 percent reduction in theft/loss/pilferage;
• 100 percent reduction in tampering;
• Up to 90 percent reduction in transit time;
• 25-50 percent improvements in on-time delivery; and
• 50 percent reduction in response time to identify and resolve in-transit problems.[2]

Far from a cost to be minimized, investments in supply chain security and resilience can pay off

(Continued on Page 8)

1. Kevin Hendricks and Vinod R. Singhal, *The Effect of Supply Chain Disruption on Long-Term Shareholder Value, Profitability and Share Price Volatility*, The Logistics Institute, (June 2005), available at: http://www.supplychainmagazine.fr/TOUTE-INFO/ETUDES/singhal-scm-report.pdf.
2. Dow Chemical, *Strategies for Supply Chain Security and Sustainability*, U.S. Resilience Project, (October 12, 2011), available at: http://www.usresilienceproject.org/workshop/participants/pdfs/USRP_Dow_CS_012312.pdf.

Workshop *(Cont. from 7)*

in terms of greater productivity and shareholder value.

3. Although Different Organizationally and Operationally, Supply Chain Security, Integrity, and Resilience Share Synergies of Solution

Security, integrity, and resilience have different objectives — and are often separated organizationally.

- ***Supply Chain Security*** protects assets — products, facilities, equipment, information, and personnel — from theft diversion, damage, and attack.

- ***Supply Chain Resilience*** mitigates the impact of disruptions — irrespective of trigger — and enables rapid recovery.

- S***upply Chain Integrity*** prevents or detects the introduction of IT functions in products, software, or systems intended to surveil, disrupt, deny, degrade, compromise, or control their performance.

These outcomes may

(Continued on Page 9)

Examples of Overlapping Tools and Best Practices for Security, Integrity, and Resilience	
Physical Security Procedures Can Help Protect Against Malware or Firmware in the Supply Chain	**Security Tools and Best Practices Include:** • Inserting security requirements in their contracts with suppliers and shippers. • Performing "boots on the ground" audits of suppliers, particularly in high-risk areas. • Installing track and trace technologies that enable them to monitor shipments and sensor technologies to be able to detect tampering. • Instituting custody controls to create accountability through the supply chain. • Investing in R&D for anti-counterfeiting anti-tampering.
Protecting the Integrity of IT Systems and Components Can Help Secure Physical Shipments	**Supply Chain Cybersecurity Tools Include:** • Securing the information systems that support supply chain resilience. • Incorporating security processes into the software development phase. • Conducting evaluations of vendors processes for quality assurance and physical and IT security. • Performing component integrity testing.
Resilience Tools Can Help Assure Viability and Security of Supplier Networks	**Resilience Tools Include:** • Providing for 24-7 monitoring of global events that could affect supply chain security. • Mapping the supply chain network to identify single points of failure, supplier financial health, and vulnerabilities to disruption. • Creating risk modeling tools, data sets, and crisis playbooks to assist both in risk planning and recovery.

Workshop *(Cont. from 8)*

be different functionally, but there are synergies of solution between them. Good physical security and chain of custody controls also help narrow the scope of cyber risks by preventing insertion of Trojan Horses in the supply chain system — or at least detecting any tampering with the cargo box or goods in shipment or in warehouses. Security procedures also help to discover counterfeit items by authenticating product bar codes or creating unique identifiers.

In the same way, tools for resilience are intended to create transparency down the supply chain tiers to enable risk managers to: identify single points of failure; test for supplier financial stability; and audit supplier processes for security and business continuity. Knowing who the lower-tier suppliers are and scrutinizing their processes is fundamental to assessing supplier risks in physical and cybersecurity.

There are efficiencies to be gained by exploiting synergies between these separate tools sets that seek to assure continuity of supply, the security of supply chains, and integrity of products and information in them.

4. An End-to-End Approach to Supply Chain is Critical to Exploit Synergies of Solution and Achieve Greater Efficiency

Threats to the smart grid can come from a number of access points in the supply chain. A "cybersecure" supply chain must be organizationally end-to-end, engaging a range of operational groups. For example:

- R&D/Technology groups can bake cybersecurity into the design of hardware and software — and make it difficult to insert malicious functions.

- Supply chain security professionals can require chain of custody controls and "track and trace" technologies that prevent or detect tampering with a component during shipment.

- Supply chain security professionals and purchasing groups create trusted supplier networks and follow-up with boots on the ground audits.

- Anti-counterfeiting teams combat brand theft inside and outside the supply chain.

The problem is that many of the functions that touch the supply chain do not communicate and cooperate well. Supply chain professionals understand how to secure the products in transit, but they are not responsible for securing the integrity of electronic components or software in the supply chain. IT professionals are responsible for supply chain cybersecurity, but they are less familiar with the security procedures that make supply chains "tamper-evident" or with quality assurance programs that could detect the insertion of unwanted IT functions.

In a complex and interconnected world, risks cascade across silos. The lack of communication and cooperation between silos can result in tunnel vision — a failure to prepare for known risks and missed opportunities to capitalize on tools and practices deployed in other silos.

5. Government and Industry Are More Aligned Than They Sometimes Appear To Be

Government and industry have different languages, different perspectives, and different missions that obscure real intersections of interest.

Differences in Language: Government often thinks in terms of threats and vulnerabilities. For businesses, a focus on vulnerabilities, rather than risk mitigation, impedes partnerships. Not all vulnerabilities have significant consequences, but neither can every potential vulnerability be fully mitigated — the cost would be prohibitive. The focus on vulnerabilities is particularly acute for the smart grid. With potentially millions of embedded IT devices on the smart grid, the task of securing the smart grid and smart grid supply chains would be herculean. What is needed is a framework to prioritize which devices pose the greatest systemic risk, which in turn justifies the expense of extra security for high-priority parts.

Differences in Perspective: Given that government is charged with handling national level events, it often focuses on preparing for extreme events. By contrast, businesses typically focus on a

(Continued on Page 21)

Framing the Issues: Building Bridges between OT, IT, and Supply Chain

by Ed Goff, CISSP Enterprise Architect IT&T Security, Progress Energy

Executive Summary

Why is cybersecurity important to smart grid technologies or supply chain issues? When will the security requirements be complete? How closely do the stakeholders need to work together to be successful? When is cybersecurity achieved? Progress Energy's smart grid initiatives (called EnergyWise) challenge the normal approaches and work practices of operations technology (OT), information technology (IT), and supply chain experts. This challenge is being met through more frequent and better collaboration and improved processes and technology. To be successful, we realized we needed more focus on interoperability standards, enterprise architecture, and procurement processes. Goals included increasing reliability and resilience while also reducing the risk of stranded investments. As a result of these improvements, we are better able to adequately secure new grid technologies.

Fundamentally, we would like to see voluntary adoption of certain minimum security controls and standards to drive maturity in the technologies we are procuring and implementing. We would like to level set the supplier community so we can get beyond the "you're the only customer asking for this or that control and/or standard" discussion. We can all agree there are differences between the utilities deploying smart grid technologies. There are many valid reasons for these differences, not the least of which are the lifecycles of much of the infrastructure deployed and the regulatory model which we operate within. Bottom line, the utility asset owners are responsible for providing safe, reliable, and secure power for our customers and our Nation. Those responsible for critical infrastructure protection (CIP) take this responsibility very seriously. However, we cannot be successful without partnerships and collaboration with the supplier community.

This paper is aimed at sharing some of our experiences and maturity as we implement numerous smart grid technologies.

Background

Progress Energy's EnergyWise initiatives leverage existing program/project management organizational structures, standards, and disciplines to manage for on-time, on-budget delivery while ensuring benefits realization. This includes the following activities and business drivers:

- Deploy Advanced Metering Infrastructure (AMI) that establishes a scalable platform for cost effective Advanced Meter Reading (AMR)-AMI migration and positions for dynamic rates.

- Deploy grid management functionality that replaces emergency voltage reduction with utility-side demand response capability for routine operational use.

- Deploy monitoring capability to critical transmission infrastructure for asset and demand management functionality.

- Deploy feeder automation to advance partial restoration capabilities.

- Build an advanced analytics engine that forecasts, coordinates, and models a comprehensive view of Smart Grid energy and efficiency capabilities.

The initiatives include a wide range of smart grid technologies. Figure 1 (see Page 11) is a list of the initiatives that challenged the normal approaches and work practices of OT, IT, and supply chain professionals. Progress Energy's fundamental approach to cybersecurity leverages a simple defense-in-depth architecture, including the principles of "least privilege" and default "deny access" controls. Through ongoing threat monitoring activities (including some paid threat monitoring and

(Continued on Page 11)

Progress *(Cont. from 10)*

alerting services), we know that cybersecurity threats continue to increase in number, complexity, and level of impact. At the same time, business needs are driving requirements for increasing access and interoperability across enterprise applications, process computing environments, enterprise networks, and the internet. These requirements are rooted in the need for sharing of data as a business enabler and increased leverage of automation and intelligent technologies being implemented. Many times these business needs are in direct conflict with security objectives, presenting unique challenges and driving the need to better leverage our existing risk management methodology. This business-risk balanced approach required further maturity of our risk management lifecycle so that more risk evaluation was performed during product selection, implementation, and post deployment.

The OT and IT collaboration is largely education and awareness of each other's perspective, so together the resulting solution best meets the business needs. This alignment of skills drives thorough evaluation of the requirements, product capabilities, and integration needed to provide the right capability for the business. To ensure communication and coordination, we developed a new Enterprise Architecture Review Process and created a committee made up of OT and IT architects and engineers to provide standards, guidance, and governance to our project teams. These formal reviews (gates) require specific artifacts and documented follow up of issues, questions, and resolution of outstanding items. The success of this process has been so positive some project teams are even soliciting "pre-gate" reviews aimed at achieving understanding, guidance, and consensus of the architecture committee earlier than required in the formal process.

Figure 1: Progress Energy's EnergyWise initiatives.

Grid Slide Advanced Capabilities & Enhancements	Customer Facing Capabilities & Interface
• Carolinas - Distribution System Demand Response (DSDR) • Florida - DSDR Phase 1 • Condition Based Monitoring • Feeder Segmentations	• AMI • DLC Switch Uplift • Plug-in Hybrid Electric Vehicles • Residential Program Development and Offerings
Underlying Systems Infrastructure • Mesh Neighborhood Area Network (NAN) • Underlying Architecture Development • Other Telecommunications	

The OT, IT, and supply chain collaboration ensures that the right foundational capabilities (e.g., network security, authentication, monitoring, configuration management, etc.) are in the procured component or solution. Our Supply Chain Operating Framework includes specific collaboration in the following areas: purchasing, contracting, category strategies (roadmap and strategy sharing), supplier management, and performance monitoring. There are many supply chain vulnerabilities we intend to mitigate through these enhanced processes and increased collaboration. Hardware integrity during manufacturing includes issues from chip integrity to (digital) birth certificates used in the initial setup and provisioning of new intelligent components as trusted hosts. Poor practices and inadequate planning of the deployment phase could introduce incomplete and/or incorrect implementation configurations, leaving components at risk. There are countless possibilities of substitution of corrupted components in transit, warehouses, and with distributors. Without adequate security controls, testing, and verification, IT functions intended to surveil, disrupt, deny, degrade, compromise, or control the performance of a product or system could be introduced. Accidental quality defects, or worse case, intentional corruption of components and systems intended to degrade, compromise, or control the system create vulnerabilities through embedded malware, backdoors, Trojans, etc. Poor coding practices and inadequate testing result in application vulnerabilities that could be avoided (e.g., Open Web Application Security Project Top 10, 2011 CWE/SANS Top 25 Most Dangerous Software Errors, etc.)

(Continued on Page 12)

Progress *(Cont. from 11)*

Why Is This Important Now?

The importance of ensuring the right security controls are achieved in these components and solutions is not new and did not start with the deployment of smart grid technologies. There is greater awareness and understanding of these issues now, but the industry trends are more than a decade old. These include:

- Evolution from manual and analog to automated and digital components and solutions;
- Increase in components with built-in advanced connectivity capabilities and more intelligence;
- Needs for remote access for support staff;
- Increased use of customer information including 3rd parties and hosted situations; and
- Offshore development and new suppliers who are unfamiliar with our industry and our reliability needs.

New suppliers to the electric industry present the biggest challenge. Many new suppliers are not familiar with the level of safety and reliability demanded from the electric industry or its responsibility to its customers and to the Nation. As a result, components and solutions are being developed with nonexistent and/or inadequate built-in security capabilities and without accounting for applicable interoperability standards.

Supply Chain: Things Happening Now

There are many drivers for this increased emphasis on supply chain vulnerabilities and needs for greater collaboration among OT, IT, and supply chain professionals. The Chertoff Group and Edison Electric Institute recently published *U.S. Investor Owned Utilities Top Threat Scenarios and Mitigation Actions*, highlighting the likely target types and specific attack paths for supply chain disruption or compromise, including:

Likely Target Types:
- Unique and hard to rapidly manufacture parts, equipment, and supplies; and
- Commonly used hardware, firmware, or software.

Specific Attack Paths:
- Resulting from deficiencies in 3rd party support or vendor management:
  - o Compromise of software or firmware;
  - o Unknown 3rd party relationship chain;
  - o Exploitation of 3rd party hosting of critical systems (e.g., data centers); and
  - o Control service provider compromise.

Smart Grid grant recipients are under greater scrutiny to demonstrate good practices. There are specific DOE review expectations aimed at reducing supply chain vulnerabilities (e.g., risk management, testing, and supplier management/monitoring). The U.S. Resilience Project's (USRP) Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience was convened to explore how private-sector best practices in supply chain resilience and risk management can help protect the smart grid and other critical infrastructure from cyber risks. The 17th Annual Utilities Supply Managers Alliance 2012 Conference included sessions on smart grid, supply chain vulnerabilities, and risk reduction. From this conference, a new workgroup was formed with a standing agenda item to mature how utilities and suppliers address supply chain vulnerabilities. Finally, some new draft cybersecurity legislation attempts to tackle some of the larger supply chain opportunities such as supplier management and performance monitoring.

Some Good Practices

These are some good utility practices that are being leveraged to mitigate supply chain vulnerabilities in smart grid initiatives. This is not meant to be a complete list, but some of the high value ones that others are benefiting from:

- Increased positive collaboration with DOE. DOE leadership and guidance in cross industry collaboration, the ieRoadmap, intelligence community coordination, and research and development activities continue to drive mature practices and improve cybersecurity throughout the industry.

- Increased collaboration and teamwork between OT, IT, and supply chain professionals through

(Continued on Page 13)

Progress *(Cont. from 12)*

formal processes.

• Implementation of mature risk management practices throuhout the lifecycle of the initiatives, including evaluating specific actors, interfaces, dataflow, sample data, security capabilities, etc.

• Adoption of applicable interoperability standards, including specific requirements in requests for proposals and contracts, increase reliability, security, and reduce risk of stranded investments.

• Integration of the steps from the National Institute of Standards and Technology Interagency Report (NISTIR) 7628 *Guidelines for Smart Grid Cyber Security* into architecture and review processes.

• Security architecture and design are implemented to meet the intent of many of the North American Electric Reliability Corporation (NERC) CIP controls, but without the administrative overhead (e.g., network isolation, access control, configuration management, monitoring, etc.).

• Incorporation of DHS Procurement Language to Secure Control Systems in contracts and tables of compliance. This is being studied through the DOE Electric Sector Control Systems Working Group for updates, education, and awareness in the industry.

• Use of vendor/supplier questionnaires and performance evaluations to determine completeness and maturity of security capabilities and controls.

• Sharing of roadmap and strategy information with vendors and suppliers, challenging them to do the same, in an effort to align and identify improvement opportunities and product direction.

• Expectations that vendors/suppliers will proactively perform cybersecurity assessments and share executive summaries of results, including actions to prevent reoccurrence.

• Performance of privacy impact analysis to identify sensitive privacy and interval energy usage information so appropriate controls can be applied. This analysis should become a routine step in the Software Development Lifecycle and applied equally for in-house developed and procured software.

• Development and implementation of mature cybersecurity testing capabilities, including processes, tools, test cases, and traceability.

Going Forward Recommendations

These are transformational times for the electric utility industry. For that reason, there are tactical and strategic next steps to safely and securely deploy these technologies and realize the value of the smart grid.

In the short-term, we need to share tools lists, processes, and capabilities with our peers in the industry and solicit from those outside our industry. We need to continue to increase collaboration with OT, IT, and supply chain professionals, including further improvements to contract language. We need to build consensus on existing standards and good practices (e.g. Wurldtech, ISA Secure, IEC 62443, DHS Procurement Language, etc.).

Long-term, we need a quick, concise safety check for software and hardware used in critical infrastructure and control system environments. We like to call this a *Critical Infrastructure Safety Seal*. This should be based on existing standards (e.g. Wurldtech, ISA Secure, IEC 62443, DHS Procurement Language, etc.) and ideally drive some responsibility to the vendors and suppliers. We need to continue to learn and implement good practices from other industries and continue to mature the OT – IT teamwork, including skills convergence where warranted (e.g., meter alarms and security events correlation).

Public-private partnership improvement areas include stronger partnerships between DOE, DHS, the intelligence community, and utilities as well as more timely information sharing and reporting. Also, we need an appropriate distribution of clearances to facilitate adequate information sharing normally and during attacks. This distribution needs to include a good mix of operational, technical, and managerial levels needed to appropriately evaluate, respond, and make timely decisions necessary to slow or stop the attack. Ultimately, this continued collaboration with DOE,

(Continued on Page 26)

Supply Chain Security in Smart Grid Components Best Practices at Schweitzer Engineering Laboratory

by Ed Schweitzer, President,
Schweitzer Engineering Laboratory

The reliability, continuity, security, and integrity of the supply chain have never been more important — or more at risk. It is in the best interests of our suppliers, our customers, and their customers to get it right.

Schweitzer Engineering Laboratory (SEL) manufactures in the United States, which creates several supply chain advantages:

- **Shorter Lead Times:** Its U.S. footprint creates tighter supply chain communications and controls and fewer transportation issues. This gives the company an average 10 day turnaround time on orders versus a few months for many competitors.

- **Rapid Adjustment to Supply Disruptions:** The U.S. manufacturing presence facilitates fast turn-around to deal with the unexpected. For example, when a large shipment was destroyed in a freight train accident, SEL was able to reconstitute the shipment in two weeks. The capacity for fast remanufacturing not only creates customer satisfaction, but often avoids large late delivery penalties as well.

- **More Confidence in Ability to Secure the Supply Chain against Malware and Firmware and to Protect Intellectual Property:** Supply chain risk management processes have been focused on reliability and revenue. These days, the focus needs to be on protecting the integrity of supply chains as well.

SEL's Best Practices: Creating Tools for Supply Chain Security, Transparency, and Assurance

Product Database: SEL maintains a database of all products it has manufactured which helps track suppliers — where they are coming from and where they go; assure customers that the products are legitimate and have not been outside of the SEL demand chain; and fast track efforts to ramp up production to meet disruptions in the supply chain or demand spikes.

Parts Database: Creating Visibility to Evaluate Suppliers: SEL also maintains a parts information data that covers every component. It collects data on supplier manufacturing locations; where materials are fabricated, packaged, tested, and shipped; and the names of key people and contacts.

This data allows SEL buyers to respond quickly in case of disruption. In the aftermath of the 2011 Japanese earthquake and tsunami, SEL was able to quickly identify which parts were at risk and, as a result, immediately moved to purchase additional inventory from existing and alternative suppliers to ensure the uninterrupted flow of SEL products. To minimize the impact of disruptions, SEL works with its suppliers to ensure that six months of inventory is continually secured for high risk components, four months for medium risk, and three months for low risk.

Supplier Evaluation System: SEL employs a supplier risk rating system, combining risk intelligence from its R&D, supplier quality, finance, and purchasing departments to assess:

(Continued on Page 22)

SEL's Product Database Collects Information On:

- Product ID, firmware ID, and serial number
- Subassembly data and work instructions
- Who built it?
- When it was built?
- Where was it built?
- What line was it built on?
- What test station was used?
- Who bought it?
- Who is the end-user?
- How was it shipped?
- Who was the sales rep?

Best Practices in Supply Chain Security, Resilience, and Integrity

The following article is comprised of vignettes taken from various company case studies that describe a range of best practices in supply chain security, integrity, and resilience. The full case studies can be found at www.usresilienceproject.org.

Telvent: Security is Baked into Software Development

From core geospatial network modeling and management, to real-time analytics and control, Telvent builds software to enable the smart grid.

Telvent uses Agile software development — a methodology based on iterative and incremental development and collaboration between cross functional teams. Coders work in pairs for actual programming tasks. On the surface, any attempt to build disruptive or malicious functionality (malware) into the code would require at least two people working in tandem. In fact, even the coding pairs could not succeed in delivering code with embedded malware. The methodology dictates that teams never build anything that takes longer than two and a half weeks (a sprint), which could be anything from a couple of hundred to a couple of thousand lines of code. Each sprint involves at least one code review, during which members of the team "walk through" each other's code. Functionality is tested at the end of each sprint by a Quality Assurance Specialist assigned to the team, against vetted requirements. To introduce malware into an application in an Agile system would likely require the complicity of everyone on the subteam, approximately four to eight members, including the Product Owner, a senior programmer with both management and coding skills.

A second level of security is attained during the testing process. Once during each release cycle, each project team takes a one-day break in the coding cycle to stress test. This exercise (SWAT – Software With A lot of Testers) takes place at a known date prior to release, and is an all-hands-on-deck exercise in which all programmers stop coding and start testing, looking not only for quality bugs but security issues as well: holes, places in the code with a single sign-on, hard coded paths, legacy protocols, and anything that creates or increases the threat surface. The rewards are geared towards finding and learning from mistakes — and there are prizes for those who find the most bugs and the most significant security threats.

Jeff Meyers is Director of Business Development for Telvent's Smart Grid Business.

Dow: Chain of Custody Controls Narrow Risk of Counterfeit and Compromised Products

Dow's supply chain security is rooted in chains of custody controls. For certain types of products, the company has established the capability for 24-7 monitoring of the cargo's location — e.g., who has responsibility for its handling and whether there has been unauthorized entry into the containers in transit or at the points of hand-off from one party to another.

Dow began implementing a strategy for asset visibility through a combination of radio-frequency identification (RFID) tagging, global positioning system (GPS), and sensor technologies about six years ago. Although RFID had long been used to track chemical shipments by rail, the communication was one way — the container had to pass an RFID reader to signal its location — and did not cover other modes of transportation. By combining RFID and GPS technology, the company got real-time location information. Today, Dow's web-based "DowTrak" container tracking portal gives the company and customers the ability to track shipments no matter what mode of transportation or area of the world.

GPS and RFID technologies are coupled with sensors which allow supply chain managers to monitor the condition of the material and the integrity of the container. Electronic seals can monitor whether the door has been opened; whether the sensors detect light.

(Continued on Page 16)

Best Practices *(Cont. from 15)*

There are shock detectors, which can enable the company to detect where rough handling may be damaging the transportation equipment or products in the container, and humidity sensors to monitor for the presence of water vapor. Previously, water vapor was detectable only after drums deteriorated as a result of adverse conditions during ocean transits. These types of asset visibility measures serve both product quality as well as security needs.

Given the volume of shipments, it is not practical to track every shipment. Dow's focus is on cargo that is:

- **High Value**: For example, catalyst materials and agricultural chemicals which could bring a high price on the black market;

- **High Hazard**: For example, materials that are toxic to inhale which could be used as weapons of mass effect by terrorists; and

- **Highly Regulated**: For example, chemicals that could be repurposed to manufacture illegal drugs or chemical weapons or products sold into sensitive end-use markets such as direct food and pharmaceutical applications.

As the need is determined by risk assessments on products in these categories, Dow has the ability to maintain 100 percent visibility on a shipment from the time it leaves the shipping location until it arrives at its destination.

Henry Ward recently retired as the Global Supply Chain Director, Security, and Sustainability & Public Policy at The Dow Chemical Company.

Verizon: Supply Chain Security and Resilience Secure Network Operations

For Verizon, cybersecurity is not just a technology problem. Many non-cyber business practices need to be implemented to assure cybersecurity, including knowing who the company is doing business with, knowing the ownership and location of contractors and subcontractors, and ensuring validation and compliance with contract terms and conditions. These supply chain processes are just as important as testing the quality and security of devices when they arrive from manufacturers.

Verizon implements numerous security processes that help manage cyber risks in the supply chain, including the following:

Vendor Controls: Security processes are embedded into supply chain processes, from the selection of appropriate vendors and locations, to the completion and delivery of products or services, to the turndown of the relationship. Prior to any contractual agreement, prospective Verizon suppliers are scrutinized on criteria such as ownership and location; links to foreign countries; and red flag violations, including export controls. Verizon uses its own intelligence and public information to review suppliers.

Internal Clearance Processes: Verizon conducts an additional internal clearance process on prospective vendors to make sure that a business relationship is in compliance with all legal and regulatory imperatives as well as all security priorities. This process includes background checks, export control statements, requirements for off-shoring or outsourcing notification and approval, disclosure of baseline security for handling data, and other clearance requirements, including assessments of physical and cyber controls.

Risk Prioritization: Verizon prioritizes these assessments both by ranking the criticality of components and the assurance levels desired for suppliers that have access to Verizon data, products, or systems. Many of the major components are purchased from key vendors that are within a trusted category and face restrictions on where products can be developed and manufactured as well as where services may be performed. For certain relationships, Verizon contractors are required to list their subcontractors.

Assessments of High-Priority Vendors: Verizon also performs on-site reviews of high-priority vendors to ensure that they are complying with requirements and meeting appropriate security practices. Verizon employs on-site inspections and audits for these reviews; there is concern that questionnaires may create a false sense of security. Vendors often give the answer that

(Continued on Page 17)

Best Practices *(Cont. from 16)*

they think their customers want to hear or what the vendor believes is in place. Experience has shown that questionnaire answers rarely match up to the findings of on-site inspections.

Henry Shiembob is Executive Director, Cyber Security and Fraud Operations, Verizon, and James McConnell is Director of Security, Verizon.

Hewlett-Packard: Mature Supply Chain Business Processes Strengthen Security, Resilience, and Product Integrity

Hewlett-Packard (HP) has one of the industry's most extensive supply chains: more than 1,000 production suppliers (responsible for product materials, components, and manufacturing and distribution services) in more than 1,200 locations; 450 supply chain nodes; and a billion customers worldwide. HP ships more than 60 million computers, printers, and servers every year — approximately 3.5 products every second.

Supply chain security begins with a set of rigorous business processes and controls. More rigorous controls evolved in lock step with globalization. Twenty years ago, supply chain executives had more hands-on control when manufacturing and warehousing was done in-house. The globalization of manufacturing and distribution networks necessitated more organized business processes to combat corruption, quality issues, and theft. There are many processes in place to create confidence in the materials being sourced, the quality of the manufacturing process, security of the products in shipment, and end-of-life disposal.

Far from minimizing investment in supply chain risk management, HP spends roughly $60 billion annually, or nearly half of its total sales, in support of its supply chain. Every year, the company conducts an annual supply chain mapping process to identify the most critical first- and third-party exposures. It regularly exercises supply chain continuity plans and emergency response capabilities in table-top drills. It also convenes an annual Suppliers Summit, bringing together more than 500 representatives from 150 suppliers, to share vision and priorities. HP encourages its supplier base to adopt supply chain practices as well as technology solutions — and early resistance has turned into a standard part of doing business for most suppliers.

Security programs tend to differ based on product, country, and regional risks; HP suppliers have adopted much more stringent security measures in higher risk areas. HP conducts about 100 audits of its supply chain partners every year — with follow-up action to ensure that corrective measures are implemented. Sites are selected for audit based on product value, volume, and risk.

Fred Smith is Director, Supply Chain Global Security Group, HP.

Cisco: Supply Chain Resilience is Integral to Risk Management

Cisco has built a risk management program focused on anticipating and mitigating any event or circumstance that could disrupt its global supply chain. Cisco's supply chain risk management process pairs risk intelligence — knowing where their vulnerabilities are — with risk analytics — knowing where the highest probabilities for disruption are located.

Key tools for supply chain risk management include:

Business Continuity Planning (BCP): Collects information on key suppliers and key nodes in the supply chain. Business continuity data gives Cisco insight into the impact of a disruption, creating an ability to identify which suppliers are affected by an event and its overall impact on the supply chain.

BCP Visualization: Cisco's BCP Visualization capability provides a way to quickly assess the impact of an event — identifying which supply chain nodes are in the affected region, what parts and/or products are made there, and what alternate sites can/should be engaged. This visualization and the underlying data becomes the starting point for any incident mitigation effort and allows Cisco to quickly qualify the potential impact an incident could have or is having on its supply chain operations.

(Continued on Page 23)

An Integrated and Collaborative Approach to Enhancing Global Supply Chain Security

by Christa Brzozowski, Director Global Supply Chain Security, National Security Staff

This past January, the Administration published the *National Strategy for Global Supply Chain Security*. The Strategy establishes two foundational goals: 1) to promote a global supply chain system that is both secure and efficient; and, 2) to enhance the resilience of the system, with the aim of improving its capacity to absorb and recover rapidly from disruptions, whatever their cause. The Strategy also defines the approach by which we will work to achieve those goals — through a strong commitment to collaboration within the U.S. government, between governments, and with industry, as well as prioritizing our efforts in accordance with an informed appreciation of risk. It is intended both to provide guidance to U.S. Federal government departments and agencies with supply chain transportation and shipping-related missions, as well as to communicate those priorities and direction with non-Federal stakeholders with related roles and responsibilities. The Strategy underscores the importance of an all-of-nation approach - recognizing that everyone can contribute to safeguarding the Nation, and emphasizes the importance of a holistic, "end-to-end" approach to supply chain management.

The Integrated Approach

The challenges we face in the interconnected and complex global supply chain system are complex and multi-disciplinary. To meet these challenges, we must develop a new approach. For example, security policies and programs not only protect goods and infrastructure, but can enhance efficiencies (by providing better insight into supply chain processes), and speed commerce (by focusing extra attention only on those high-risk shipments that require additional scrutiny). In the same way, resilience tools that promote a safer, more robust system that can withstand and recover quickly from disruption can also create transparency to identify potential points of failure, test for supplier financial stability, or provide business continuity capabilities.

It is difficult to think of a topic that involves more players (private, public, foreign, State and local), modes of transport (air, land, and sea), and diversity of threats (natural, man-made), as well as nearly every critical infrastructure sector both domestically and abroad. That is why a common vision and overarching framework is so critical. It also informs and supports the range of other supply chain-related activities being advanced by the Administration — from ongoing work in the cyber, telecommunications, government, and energy supply chains; to customs revenue, trade, and intellectual property rights enforcement concerns; to national preparedness planning strategies, and ongoing efforts to combat transnational organized crime and their exploitation of this system. The *National Strategy for Global Supply Chain Security* is not intended to supersede these other critical efforts but, rather, represents a capstone piece and serves as a "north star" to organize, guide, and support them as part of a more holistic framework.

Central to this approach is effective collaboration in three areas: within the Federal family and across all levels of government; with international partners; and with the private sector.

Government Collaboration

By working collaboratively and seeking efficiencies within the Federal family and with State, local, tribal, and territorial partners, we can both protect and increase the productivity of the supply chain system. Specific opportunities that we are looking to develop and enhance within and across government stakeholders include:

(Continued on Page 24)

Legal Insights

Are We Being Smart About Regulating Our Smart Grid?

The ongoing modernization of the power grid has resulted in an electricity sector that relies upon an evolving web of interdependent players in the public and private sectors, including local, State, Federal, and international partners. This web, as with many of its sister sectors, is being spun much faster than any corresponding regulation could possibly take shape. Some see this as a reason for stalling regulatory efforts; until the smart grid architecture is firmly established, legislation should not be enacted that could deter innovation or otherwise hamper its future potential. On the flipside, private industry, consumers, State governments, and international stakeholders all want reassurance about the basics — i.e., who is in charge, who is paying, and who is accountable if something goes wrong?

Traditionally, authority over the electricity industry has been allocated according to transmission and distribution systems. The Federal Energy Regulatory Commission (FERC) is responsible for regulating the interstate transmission system and approving standards for its reliability, set by NERC, while local distribution and end-user rates are left to the discretion of State public utility commissions (PUCs). However, some features of smart grid technology may begin to challenge this distinction.

The Energy Independence and Security Act of 2007 (EISA)[1] was the first Federal legislation to endorse smart grid modernization. It tasked NIST with developing a framework for smart grid interoperability and FERC with adopting standards based on this framework to guarantee its reliability. No one doubts that while its potential benefits are numerous, having a "smarter" grid built around information technology brings additional security risks via the cyber realm. In a Senate hearing last month, the Director of Information Security Issues at the Government Accountability Office (GAO) testified on the biggest challenges to securing the electricity sector against such threats.[2] Unsurprisingly, a main focus of his statement regarded the current regulatory environment.

Most significantly, he noted that while NIST, FERC, NERC, DHS, and DOE have all taken steps to address smart grid security, there is "a lack of a coordinated approach to monitor whether industry follows voluntary standards."[3] As part of the interoperability framework required by EISA, NIST has developed 11 cybersecurity guidelines. However, GAO evaluated these guidelines in January 2011 and found that while largely comprehensive, they did not address "the risk of attacks using both cyber and physical means."[4] NIST is still in the process of updating the guidelines to attend to these concerns.

NERC has also established eight critical infrastructure reliability standards for identifying and protecting cyber assets, approved by FERC.[5] To date, these are the only effective mandatory cybersecurity standards protecting U.S. critical infrastructure. Nevertheless, according to the Director of the

(Continued on Page 25)

1. Pub. L. No. 110-140 (Dec. 19, 2007).
2. *Cyber Security and the Grid: Hearing Before the Committee on Energy and Natural Resources*, U.S. Senate, 112th Congress (July 17, 2012) (Statement of Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office) [Hereinafter, GAO statement].
3. Ibid., 14.
4. Ibid., 12.
5. Available at http://www.nerc.com/page.php?cid=2|20.

SARMA's 6th Annual Conference

focusing on

"Professionalizing Security Risk Management"

on

Tuesday, October 30, 2012 through
Thursday, November 1, 2012

to be held at

George Mason University - Arlington Campus
Founders Hall
3351 Fairfax Drive
Arlington, Virginia 22201

For more information on Registration, Agenda, Sponsorship, please visit
http://www.cvent.com/events/6th-annual-conference-on-security-analysis-and-risk-management/fees-20a6a8a4c2be4d02b285ed1da83a46c1.aspx.

Workshop *(Cont. from 9)*

broader set of probable (rather than possible) risks. Robert Moore, Vice President for Global Security Services at HP, commented that: "[f]or the private sector, the challenge is not just coping with hazards; it's coping with constant crises. Global enterprises often find themselves managing multiple major business disruptions in different parts of the world on the same day."[3] In fact, the processes, skills, and technologies that businesses deploy to manage the risks they face every day also scale to meet the larger events with which government is concerned. A focus on capabilities and competencies, rather than specific scenarios, could help bridge that divide in perspective.

Difference in Mission: Government focuses on protecting national platforms like the smart grid and often looks to industry to help achieve that mission. The problem is no individual company can accept responsibility for an entire infrastructure. Building on the best practices and processes of companies across the smart grid sector, when taken in aggregate, could go a long way towards achieving the mission. But, the government needs to be looking to build a national solution from the bottom up, rather than from the top down. The DOE Cybersecurity Roadmaps, developed with private sector leadership, provide a model for how this can be done in smart gird supply chain security as well.

The bottom line is that the tools and best practices that global companies have developed to manage supply chain risks can inform and shape cybersecurity strategies. But, these tools are not well known or well integrated into cybersecurity planning — in government or industry. Securing the smart grid is a critical priority, but some of the best solutions are hiding in plain sight. ❖

Debra van Opstal is the Executive Director of the U.S. Resilience Project, http://www.usresilienceproject.org.

3. U.S. Resilience Project, *Priorities for America's Preparedness: Best Practices from the Private Sector*, (October 31, 2011), available at: http://www.usresilienceproject.org/pdfs/USRP_Priorities_Final_020112.pdf.

SEL *(Cont. from 14)*

• Manufacturer location risk, based upon location for all process steps;
• Supplier quality risk, based on defect data;
• R&D risk based on technology type and the length of time required for redesign purposes should the part become unavailable;
• Finance risk, based on a manufacturer or suppliers financial health; and
• Purchasing risk, based on supplier performance for on time delivery and responsiveness.

Product Integrity: SEL goes to great lengths to assure the product integrity — to ensure that what its customers get is what they have been promised.

• In addition to qualifying suppliers, all prospective procurements undergo a qualification process.

• Component purchases must be qualified by SEL's R&D group and are procured directly from the manufacturer or from officially franchised suppliers.

• SEL does not deal with brokers — and where parts are purchased outside these prescribed paths, they are routed directly into the supplier quality department where the parts are stripped down and compared to manufacturers drawings.

• Testing is done continuously and rigorously throughout the manufacturing process. Any variation in performance leads to a stop shipment call.

• One strike and you are out rule. All third party SEL suppliers work on a "one strike and you are out rule." If a 3rd party source sends a counterfeit component, or components do not meet SEL specified requirements, that supplier will be flagged in the supplier qualification database as unapproved, and SEL will not order from them again.

Product Quality: SEL offers a 10 year warranty on its products and has never charged a penny to fix, repair, or replace anything. The company created strong incentives to bring technology back so that SEL can find the root of the problem within 72 hours. If the issue is not resolved within that time frame, the product is replaced free of charge — and SEL continues to investigate on its own time. Where appropriate, a service bulletin defining the problems, risks, and remedies is issued. SEL also ages its own products and collects data to inform what it is seeing in the market. Service bulletins are also issued on this research.

Trusted Supply Networks: SEL hosts a day and a half annual conference with supplier representatives from 200 organizations to:

• Share an overview on of the company's history, values, and corporate culture;
• Describe what its products do and explain why lives depend on the quality and reliability of their products;
• Provide an overview of the industry sector and the technical market and policy forecasts;
• Share SEL's technical needs and strategic objectives for the coming year;
• Create opportunities for feedback from suppliers on what SEL could do differently; and
• Enable an environment for collaborative brainstorming and communications.

Supplier dialogues continue throughout the year in both directions. SEL employees make about 50 plus supplier visits every year to discuss new opportunities and areas for improvement. ❖

Avoid Interdiction:

- Buy and sell direct, avoid brokers
- Inspect packaging, track lot numbers
- Doubts? X-Ray, unpackage, contact
- manufacturer
- Keep inventory close
- Select shipping methods with care
- Support customer with installation and
- commissioning.
- Every failure is significant. Get to the root cause.

Best Practices *(Cont. from 17)*

Crisis Monitoring: Cisco contracts with the National Center for Crisis and Continuity Coordination (NC4) to provide round-the-clock global monitoring to achieve its goal of "sense and respond" situational readiness. Cisco has worked with NC4 to map all of its critical supply chain nodes worldwide and has set criteria for when alarms need to be sounded.

Playbooks: Cisco has developed a set of response playbooks that provide a framework for organizing an incident response team, as well as a process for assessing the ground-level impact of a disruption, translating that into an actionable set of mitigation actions and identifying potential impacts to specific products, customer orders, and ultimately to customer operations.

Resiliency Index: Cisco invented the Resiliency Index and the TTR metric because it was not able to find any pre-existing standards or metrics to meet its needs. The Resiliency Index is a composite of resiliency attributes for the key "care-abouts" at Cisco — these include product resiliency, supplier resiliency, manufacturing resiliency, and test equipment resiliency, a key control point given the globally outsourced supply chain.

James Steele was formerly Program Director, Supply Chain Risk Management, Cisco.

NASA's Supply Chain Challenge

The National Aeronautics and Space Administration (NASA) faces a significant challenge: not just assuring the security and integrity of the components in the supply chain but, given the hiatus in space operations, assuring that there is a viable industrial base at all. NASA's focus has been on creating new tools to assess how programmatic changes impact the financial liquidity of the supplier base and map the multi-functional relationships of the lower-tier suppliers in the supply chain.

NASA developed two tools to help manage supply chain risk: Prime Supplier and Prime Map.

Prime Supplier: The model identifies a number of risk indicators and creates a risk value for each. These indicators are then integrated into a framework that creates a meaningful and consistent risk value for each supplier. Prime Supplier captures risk metrics in three key areas:

- **Financial Stability Risk Indicators** include profit margin, debt-to-equity ratio, current ratio, and percent of dependence on government contracting.

- **Operational Performance Risk Indicators** include indicators for perfect order fulfillment (POF), order fulfillment cycle time (OFCT), schedule achievement, first-pass yield (FPY), and defects per million opportunities (DPMO).

- **Supply Chain Management Risk Indicators** include measures of communication, collaboration, and coordination up and down the supply chain and an assessment of supply chain practices based on a modified supply chain readiness level assessment.

Prime Map: Prime Map is a supplier mapping software application that creates a visual representation of supplier relationships across geographies and programs and an ability to compare supplier quality, performance, and risk across programs and elements. ❖

Michael Galluzzi is Supply Chain Manager, Kennedy Space Center.

Supply Chain Security *(Cont. from 18)*

modernizing and streamlining our processes and requirements; better coordinating our technology research and development priorities; advancing the development of key information sharing and analysis systems; evolving our understanding of risks to guide our allocation of resources; and supporting global standards and best practices as a means of encouraging stakeholder action.

Collaboration with International Partners

The challenge of developing and maintaining a secure, efficient, and resilient supply chain system is clearly a global concern. Governments worldwide share an interest in combating the exploitation of the supply chain by those looking to traffic contaminated or counterfeit products or other illicit contraband. We have a collective interest in protecting the supply chain against deliberate attacks or disruptions, such as international piracy or the threat of weapons of mass destruction.

Our overall vision and collaborative approach to strengthening the global supply chain in partnership with other governments is highlighted in initiatives such as the *U.S.-Canada Beyond the Border Initiative*, the *21st Century Border Management Initiative* with Mexico, our renewed emphasis with the European Union on a range of supply chain security and economic competitiveness issues, and continued work with regional forums such as the Asia Pacific Economic Cooperation. These inter-governmental partnerships, to just name a few, underscore our commitment to developing collaborative solutions that simultaneously streamline procedures for customs processing and regulatory compliance; align and mutually recognize security programs; and create opportunities to modernize infrastructure and expand capacity.

Collaboration with the Private Sector

The public and private sectors share common objectives. At the company level, supply chain efficiency, security, and resilience is becoming a competitive differentiator. Economic vitality, powered by global trade and our supply chains, is a fundamental pillar of our Nation's security.

Protecting the global supply chain is a shared responsibility. No one in either the public or the private sector has the resources, the authorities, or the full range of expertise to address this problem in isolation. By understanding what needs to be done, we can together assess which stakeholder is best positioned — and has the systems expertise, competencies and tools, trained workforce and resources — to do it. In many cases, this will mean that government must look to encourage, rather than require action, while in others situations government leadership and direction will be necessary.

As the U.S. Government looks to implement the *National Strategy for Global Supply Chain Security* and other efforts, industry voices will be critical to help inform the dialogue and identify areas for action and attention. We continue to rely upon the Federal Advisory Committee Act process as well as established mechanisms for private-public collaboration within and across the numerous domestic critical infrastructure sectors (such as the Critical Infrastructure Partnership Advisory Committee).

The economic prosperity of nations worldwide is dependent upon this vital system. It takes a community of effort to safeguard its security, improve its efficiency, and strengthen its resilience. We have established a common vision with the *National Strategy for Global Supply Chain Security* to enhance collaboration among U.S. departments and agencies and to also guide our interactions with key partners. Throughout the implementation of this Strategy and numerous others on related topics, we will look to develop innovative, risk-informed solutions that best leverage expertise and experience both within and beyond the Federal government. ❖

Legal Insights *(Cont. from 19)*

FERC Office of Electric Reliability, "the identification of critical assets is the cornerstone of the CIP standards" and they currently give utilities "significant discretion" to make that determination.[6] FERC has approved a new version of the standards that includes a more concrete definition of a critical asset, but it will not go into effect until 2014. In its *Smart Grid: Ten Trends to Watch in 2012 and Beyond*, Pike Research criticized the lengthy NERC/FERC standard development and approval process, claiming "it appears that this is an industry that does not collaborate well."[7] FERC has yet to adopt any smart grid cybersecurity standards based on the NIST interoperability framework as intended by EISA, asserting "insufficient consensus to do so."[8]

While FERC has authority to adopt and enforce cybersecurity standards in order to ensure the reliability of the bulk transmission system, DHS is the lead agency responsible for protecting critical cyber resources across all sectors. Within this capacity, it manages the National Cyber Security Division's Control System's Program, which publishes recommended practices to control systems operators, such as those listed in its *Catalog of Systems Security: Recommendations for Standards Developers*.[9] The program also runs the Industrial Control Systems Cyber Emergency Response Team that provides on-site support and real-time intelligence and analysis. In addition, DOE, in charge of organizing public-private partnerships across the energy sector, recently released the *Electricity Subsector Cybersecurity Risk Management Process*, designed "to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector."[10]

Clearly there are plenty of agencies, commissions, policies, standards, guidelines, programs, and frameworks attacking the problem. Nonetheless, there remains a lack of cohesion and coordination across and among government and private stakeholders. The GAO recommends that a process be developed whereby "the extent to which utilities and manufacturers are following voluntary interoperability and cybersecurity standards" is periodically evaluated.[11] Yet the FERC Chairman, though agreeing with the recommendation, felt that "coordinated monitoring of compliance with standards would be premature at this time," citing the "lack of sufficient consensus for regulatory adoption" as well as "the continuing evolution of standards."[12]

The FERC Chairman may not be wrong. Smart grid architecture is still developing. Premature legislation or regulatory efforts could be detrimental and should not be undertaken without due consideration of long-term implications. We cannot stay on this merry-go-round forever. Both the GAO and outside reports indicate that utilities will not invest in security that is not mandatory, particularly if they fear a new regulation might later require something different.[13] They, as well as every other stakeholder, need to know what is expected of them and that someone has the power to ensure compliance. Otherwise, Pike's 2012 observation that "Cyber Security Failure Risks Inevitability" will remain true, and unfortunately, "[t]he best hope for a wide-scale deployment of cyber security in smart grids is actually a successful large-scale attack that gets everybody's attention."[14] ❖

---

6. *Cyber Security and the Grid: Hearing before the Committee on Energy and Natural Resources*, U.S. Senate, 112th Congress (July 17, 2012) (Statement of Joseph McCelland, Director, Office of Electric Reliability, Federal Electric Reliability Commission).
7. *Smart Grid: Ten Trends to Watch in 2012 and Beyond, Pike Research*, (2012), 8, available at: http://www.pikeresearch.com/wordpress/wp-content/uploads/2012/03/SG10T-12-Pike-Research.pdf.
8. GAO Statement, 13.
9. Available at http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf.
10. U.S. Department of Energy, (May 2012), 9, available at: http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf.
11. GAO Statement, 18.
12. Ibid.
13. GAO Statement, 16; Pike Research, 8.
14. Ibid., 8-9.

Smart Grid Security *(Cont. from 5)*

reducing vulnerabilities in devices and communications, increased risks to the smart grid will come through the supply chain. The workshop on best practices in supply chain security, integrity, and resilience brought together public and private sector executives to catalyze a dialogue on how to address this problem, the extent to which private sector best practices could help narrow supply chain risks to the smart grid, and identify gaps that could be filled by public-private partnerships.

Nearly 100 supply chain risk managers from the power, aerospace, chemical, information, and manufacturing industries came together with government officials and national lab and academic researchers to identify industry best practices and recommendations for the future.

The Workshop will help manage the risk of compromised, counterfeit, or corrupted software or hardware in the smart grid supply chains. The remaining articles in this issue showcase some of the key themes and best practices that emerged from this initial visioning process. ❖

Progress *(Cont. from 13)*

DHS, and the intelligence community needs to provide utilities with specific, actionable intelligence in the form of "tear lines" important for detection, containment, and other mitigating tactics. ❖

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1