U.S. Resilience Project

Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices

SUPPORTING ORGANIZATIONS

Edison Electric Institute

EnergySec

George Mason University

Gridwise Alliance

Internet Security Alliance

Supply Chain Risk Leadership Council

From the Executive Director

On behalf of the U.S. Resilience Project (USRP), I am pleased to release *Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices*.

The USRP was launched in 2011 with two core insights:

- First, the best practices that businesses are deploying to manage risk also serve national missions, and national strategies should be building on these business practices.
- Second, public-private partnerships must be two-way. Private sector voices and best practices will be critical in clarifying roles and responsibilities, and increasing the leverage and effectiveness of partnerships.

We applied these two principles to an issue that has been receiving national attention: the possibility that corrupted, counterfeit or compromised components could enter the smart grid supply chain and cause serious, large-scale disruption.

In March of 2012, nearly 100 supply chain managers, IT and cybersecurity executives from a number of sectors — including the power, electronics, software, telecommunications, chemical, defense industrial base, aerospace, and heavy manufacturing industries — participated in a workshop to:

- Capture cross-sector best practices, processes, metrics, technologies and governance structures in supply chain;
- Assess how current and emerging private-sector best practices could reduce the risks to the smart grid; and
- Identify gaps and opportunities for collaborative problem solving.

Prior to the workshop, participants received executive-level briefing materials summarizing the results of seminal studies and articles on the new landscape of risk, with special sections on cyber risks, counterfeiting, new strategies for supply chain risk management, and U.S. and EU smart grid risk management strategies. Additionally, best practice case studies from a number of companies, including Verizon, Dow, DuPont, Cisco, HP, and Telvent, highlighted industry approaches to supply chain security. Finally, a number of organizations provided tools and methodologies for supply chain security — both physical and cyber. These, along with the keynote presentations, can be found at *www.usresilienceproject.org*.

The insights gleaned from the facilitated dialogue, best practice case studies, and risk management tools enabled the USRP to identify where strong solutions already exist, assess needs for more action, and identify high priority areas for public-private partnerships.

I would like to thank our workshop sponsors, the U.S. Department of Energy and George Mason University, for supporting this work. We also appreciated the support of our partner organizations: Edison Electric Institute, EnergySec, Gridwise Alliance, Internet Security Alliance, and the Supply Chain Risk Leadership Council.

I would like to thank USRP Senior Advisor Denise Swink for her strategic insights and advice, and Katie Jereza, our program manager from Energetics, who was instrumental in making the workshop a success. Dana Martin and Shannon Hayes were also an invaluable part of the USRP team.

Debra van Opstal
Executive Director
U.S. Resilience Project

Supply Chain Solutions for Smart Grid Security: Building on Business Best Practices

Debra van Opstal
Executive Director, U.S. Resilience Project

Contents

TAKE-AWAYS

The integration of information and communications technologies throughout the power grid is revolutionizing the way electricity is delivered and used. The problem is that embedded IT devices throughout the system also create new sets of cyber risks

Finding ways to manage these risks — physical as well as cyber — is increasingly urgent for both economic competitiveness and national security. When the electricity does not work, neither does almost anything else.

The cybersecurity of the smart grid is not only an IT problem, it is also a supply chain problem. At each phase in the extended supply chain — from product design, manufacturing quality, secure transportation, warehousing, maintenance and repair through secure end-of-life disposal — there are risks that counterfeit products or compromised components could be inserted into the smart grid.

Supply chain risks to the smart grid are growing because the new technology is globally sourced and new vendors to the sector are not always familiar with the security and reliability needs of critical infrastructure systems with 30-year life spans. There is also the prospect of targeted international attacks via the supply chain.

Best practices of the global leaders in supply chain risk management could help reduce cyber risks to the smart grid. Over the past decade, a number of companies have developed more sophisticated processes to assure confidence in the integrity of globally sourced materials, protect physical assets and IP from theft, reduce counterfeiting, and ensure continuity of the supply chain in times of crisis.

Participants of the Security the Smart Grid Workshop in March 2012 recommended:

Benchmark and Share Business Best Practices

Supply chain best practices in security and resilience need to be benchmarked and shared with the power sector. These practices need to be explored and explained in dialogues between IT and supply chain professionals, and between utilities and their suppliers.

Clarify Roles and Responsibilities in Public-Private Partnerships

Smart grid cybersecurity is a shared responsibility that requires public-private partnerships. Partnerships can only be effective if roles and responsibilities are clarified not by what needs to be done, but who has the expertise to do it. In many cases, the supply chain expertise, competencies and tools to maintain the security, integrity and continuity of the smart grid supply chain reside with the private sector.

Prioritize System Risks

Sophisticated supply chains prioritize risk in order to allocate the most stringent scrutiny and security to the highest priority components. This kind of risk framework is also needed for the smart grid supply chain. With potentially millions of IT devices on the grid, it is not feasible to give each of them the same level of physical and cyber scrutiny and security. The framework should enable a tiered system of risk-based security measures, which provide the full measure of protection where there are system-wide, extended impacts.

Co-Invest in Technologies

One way to increase the security and resilience of the smart grid is to make the supply chain smarter. Workshop participants identified a number of candidate technologies for public-private co-investment that would simultaneously improve supply chain risk management for companies and help assure the integrity of the smart grid supply chain for the country.

Foster Common Understandings of Challenges and Solutions

Diverse stakeholders — from IT and supply chain risk managers to CEOs and boards to public utility commissioners and state legislators — often do not agree on the nature of the problem or their respective roles in a path forward. Participants stressed the need to articulate the challenges, explain the potential roles for different stakeholders, and present information in ways that encourage joint ownership of the solution.

Leverage Synergies of Solution

The use of cyber binoculars sometimes narrows the search for effective risk management tools. Tools, practices and processes that strengthen physical security and supply chain continuity can also help narrow cyber risks, but are often not seen as part of the cyber toolkit.

Augment Professional Knowledge and Skills to Support Cybersecurity Solutions

Managing cyber risks across the supply chain touches many disciplines — scientists and engineers, manufacturing and quality assurance professionals, information technology managers, procurement and logistic executives, anti-counterfeiting and distribution specialists, and operations managers, to name a few. These professionals need to know that they are part of a cybersecurity strategy — and gain new knowledge, skills and tools that enhance their ability to manage cyber risks.

Section 1: Overview
Emerging Risks and Supply Chain Solutions

The Upsides and Downsides of Being "Smart"

The integration of information and communications technologies throughout the power grid is revolutionizing the way electricity is delivered and used. What makes the new grid "smart" are the two-way connections between devices — which makes the system more agile, adaptive and able to sense and pre-empt potential disturbances; gives customers more ability to respond to market signals; and gives the country the ability to integrate renewable sources of energy.

The problem is that embedded IT devices throughout the system also create new sets of risks from:

- **Increased access points:** Tens, potentially hundreds, of millions of devices on the system with two-way communications capabilities create access points to the grid which could be exploited.
- **Interconnectivity:** The smart grid will link disparate networks, making it susceptible to vulnerabilities of other networks and creating a bridge for malware to cross from one network to another.
- **Complexity:** The increasing complexity of the system creates opportunities for failure, even without a malicious trigger.
- **Common computing technologies:** Since the grid will depend on commercial technologies, many of the problems that exist in the office computing environment (viruses, worms, Trojans, rootkits) will affect the smart grid.
- **Automation:** The smart grid will automate many manual functions, compounding the potential impact of operator error.

These new risks create challenges to the security, reliability and resilience of what is arguably the most critical backbone infrastructure. Finding ways to manage these risks — physical as well as cyber — is increasingly urgent for both economic competitiveness and national security. When the electricity does not work, neither does almost anything else: financial, transportation, telecommunications, water and sewer networks all depend on electric power at some point in their production or delivery cycle. Virtually every retail cash register, every gas pump, every cell phone, every computer and electric car depends on a hot plug. The defense infrastructure relies on the power grid for the long-term continuity of operations, which creates a national security imperative to secure the smart grid against cyber threats.

Smart Grid Cybersecurity Demands Supply Chain Solutions

Many people think of cybersecurity as an IT problem — creating the right defenses against attack, denial of service and system infiltration. That is not wrong, it is just not the whole story. Cybersecurity also depends on supply chain security to prevent the insertion of counterfeit or compromised components into the system. The end-to-end supply chain extends from technology development and design to manufacturing quality assurance to secure shipment and end-of-life disposal — and there are potential cybersecurity problems at every stage in that lifecycle.

For example, rogue code could be inserted into the software long before devices are connected — or kill switches or back doors could be built into the hardware to enable remote access which could both steal data and disable the system. Counterfeit items, which can degrade system performance, enter the supply chain in transit, in the warehouses and in distributions centers. Maintenance and repair activities — software upgrades and equipment services — whether onsite or done remotely, create opportunities to corrupt or compromise systems. And faulty end-of–life disposal can create new counterfeiting opportunities.

Although the power industry has decades of experience in assuring reliability in purchases of electrical equipment, the acquisition of "smart" components for the grid has created new challenges — the need for increased scrutiny of global IT vendors and managing the performance of a new set of component suppliers, who may not be familiar with the security and reliability requirements of systems with 30-year life spans.

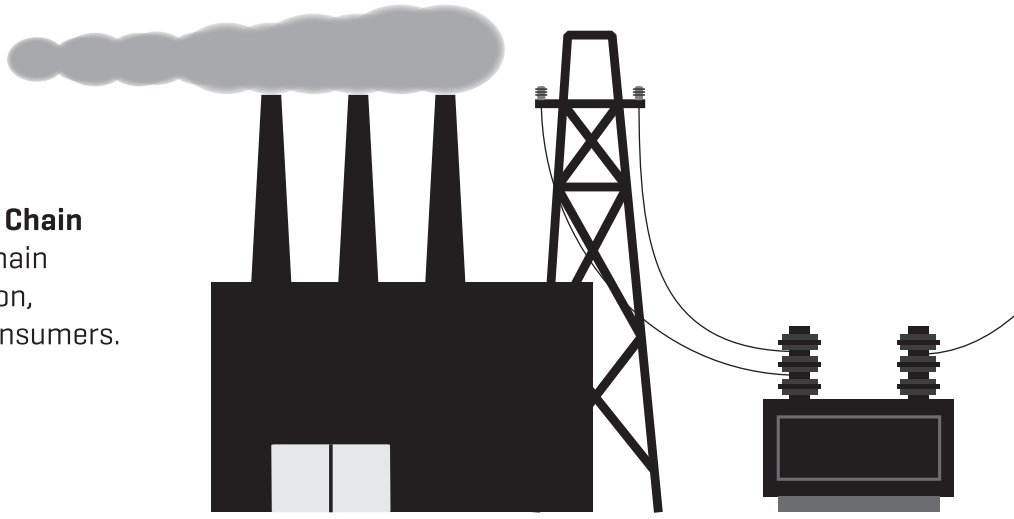
Another challenge is the lack of communication and coordination among the functions that touch supply chain cybersecurity. For example, supply chain professionals understand how to establish a secure chain of custody, but are not typically part of the cybersecurity strategy. IT professionals typically lead cybersecurity strategy, but are often unfamiliar with the security procedures that make supply chain "tamper-evident" or with quality assurance programs that detect the insertion of unwanted IT functions.

Organizational silos are causing blind spots both to emerging risks and opportunities to capitalize knowledge, practices and tools, even within the same organization.

A third challenge might be definitional. The utility industry defines "supply chain" as connections between three pillars: generation (power plants); delivery (transmission and distribution networks); and customers (residential, commercial, industrial, military, etc.). The smart grid only added advanced IT capabilities — and bi-directional communications — to those connections. As a result, when power experts hear the phrase "supply chain cybersecurity," they think about the security of the information and communications flowing between power plants, transmission and distribution systems, and consumers.

But, the risk of compromised or counterfeit electronic components — the so-called "Trojan Horse" problem — emerges out of a very different perspective of supply chain. In this view, supply chain security — both physical and cyber — is focused on managing the processes and vendors involved in moving a product from its basic components through production, assembly, shipment, warehousing and distribution. (Illustration on pages 6-7 demonstrates these perspectives).

End-to-End Smart Grid Supply Chain

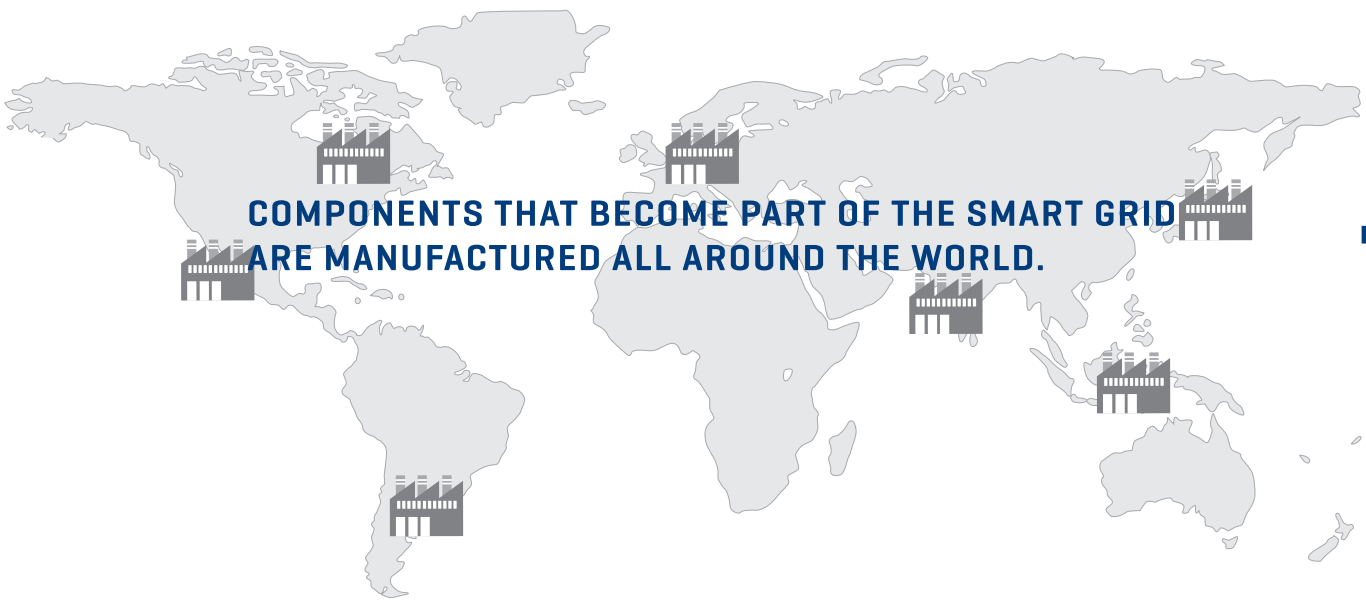


Power Sector Perspective of Supply Chain
The power sector defines its supply chain as the connections between generation, transmission and distribution, and consumers.

The smart grid added bi-directional communications and information flows into this supply chain.

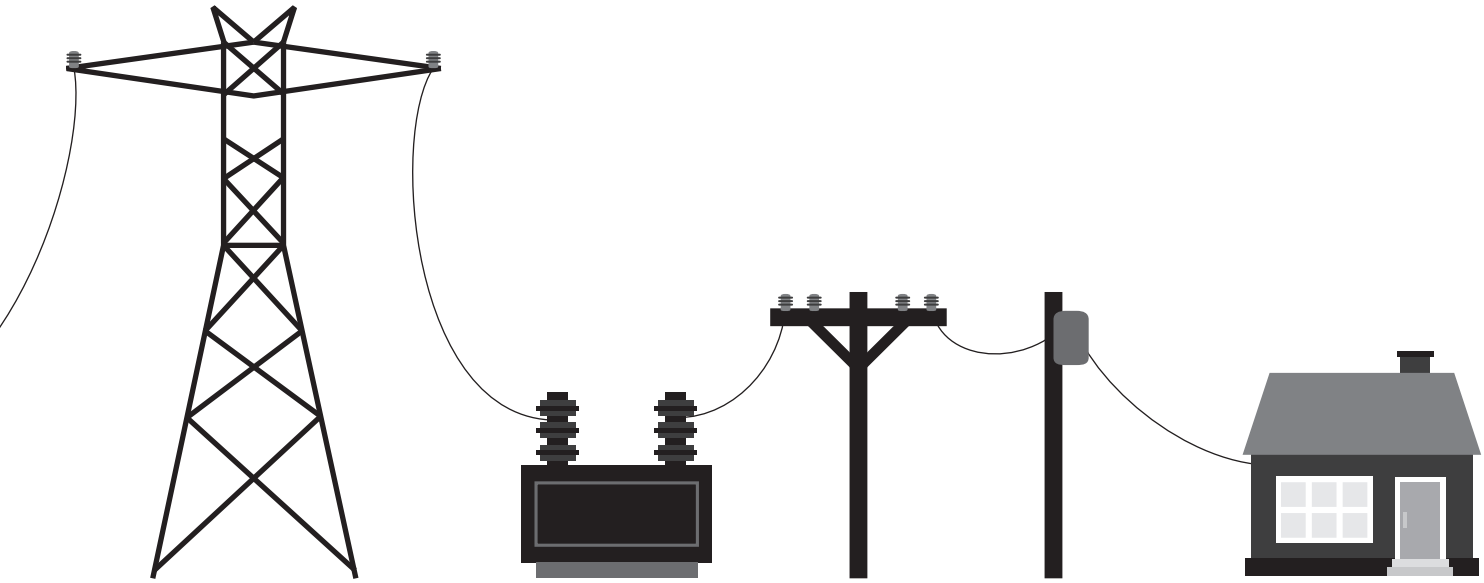
Distributed Management Systems

Advanced Metering



COMPONENTS THAT BECOME PART OF THE SMART GRID ARE MANUFACTURED ALL AROUND THE WORLD.

This simplified depiction of the smart grid supply chain describes the tiers of vendors — and thousands of companies — that produce the systems, components, subcomponents and software for the smart grid.



Supply chain cybersecurity problems stem from the risk that compromised or counterfeit components could enter the chain from lower tiers, which are less visible to the utilities.

Low visibility / high risk — **VISIBILITY TO END-USER** — High visibility / low risk

THIRD-TIER SUPPLIERS

Subcomponents
- Integrated Circuits
- Cable and Wire Harness
- Printed Circuit Boards
- LEDs
- Digital Storage

SECOND-TIER SUPPLIERS

Components
- RTU/PLC
- Meters
- Sensors
- Intelligent Electronic Devices
- Hard Disk Drives

FIRST-TIER SUPPLIERS

Major Systems
- Communications Systems
- Control Systems
- Software & Design Integration

Building on Business Best Practices to Secure the Smart Grid:

A key finding from the Workshop is that some of the best cybersecurity solutions are hiding in plain sight. Benchmarking against the best practices of supply chain leaders could provide access to new risk management tools that reduce the risk of counterfeit or compromised components in the smart grid.

Over the past decade, there have been tremendous advances by corporate leaders in supply chain risk management. Longer supply chain lines, often with less trusted partners, created new challenges — from abrupt disruptions to quality failures to IP thefts — with demonstrably negative impacts on sales, revenues, brand reputation and shareholder value. These new risks transformed supply chain problems into bet-the-bottom-line risks, with compelling incentives for investment in security and resilience.

Market Drivers for Investment in Supply Chain Security and Resilience

Cost of Disruptions	Companies that announced a supply chain disruption experienced a 9 percent drop in share prices. Two-thirds of companies still lagged their peers a year after the disruption.[1]
Cost of Counterfeits	Annual losses for electronics estimated at $100 billion.[2]
Loss of IP	Increasingly at risk in global sourcing arrangements and contract manufacturing.
Cost of Cargo Theft	Annual losses estimated at $15-30 billion in the United States alone.[3]

1. *From Vulnerable to Valuable: How Integrity Can Transform a Supply Chain*, Price Waterhouse Coopers, December 2008. http://www.pwc.com/en_US/us/supply-chain-management/assets/pwc-sci-112008.pdf.
2. Electronic Components Industry Association, http://www.eciaonline.org/councils/advocacy.aspx.
3. FBI, *Inside Cargo Theft*, November 12, 2010, http://www.fbi.gov/news/stories/2010/november/cargo_111210/cargo_111210.

In March of 2012, the U.S. Resilience Project convened nearly 100 supply chain management and IT and cybersecurity executives from a number of sectors — ranging from power, electronics, software, telecommunications, chemical, defense industrial base, aerospace, and heavy manufacturing — to explore two questions:

- What best practices in supply chain security, product integrity and continuity could help reduce cyber risks to the smart grid?
- What are the next steps to leverage supply chain best practices in support of smart grid cybersecurity?

The best practices identified by Workshop participants that could help secure the smart grid included:

End-to-end risk management practices. It would be hard to think of a risk that spans more functional specialties and stakeholders than cybersecurity. Global supply chain leaders manage risk end-to-end with integrated cross-functional teams.

Risk-based frameworks. Supply chain leaders prioritize risks based on potential impact and use that risk framework as a guideline for determining security needs.

Visibility down the supply chain tiers. Known suppliers and trusted networks are some of the strongest protections in global supply chains. Supply chain leaders have developed vendor management practices that identify, vet, qualify and audit suppliers.

Information systems to provide real-time decision-making tools. Supply chain leaders have invested in information tools — data analytics, simulation, visualization tools — that mitigate the impact of unexpected events of unknown duration and impact.

Chain of custody controls. Supply chain leaders invest in secure hand-off procedures and GPS/sensor capabilities to create asset visibility and tamper-evident shipments.

Stringent anti-counterfeiting policies and procedures. Supply chain leaders reinforce anti-counterfeiting procedures with training, new technology and constant communications with vendors, shippers and customers.

Secure design principles and ongoing testing. Supply chain leaders focus on product integrity from the outset, reinforced by secure software development methodologies, quality assurance standards and processes, and ongoing testing.

These kinds of commercial supply chain practices can go a long way toward preventing the insertion of under-performing, counterfeit or corrupted devices into the smart grid. But, they are not well known or well integrated into cybersecurity planning for the smart grid.

However, these practices cannot provide a complete solution for the smart grid supply chain. The possibility of cyber attacks by foreign adversaries via the supply chain takes the problem beyond the boundaries of a business case. Although the government may be able rely on best practices for a 75 percent solution, market forces alone cannot justify the cost of defending the supply chain against international cyber attacks. Government must help develop the advanced tools, global awareness and strategies to help defend utilities and the smart grid supply chain against sophisticated cyber threats and be ready to share information on the evolving threat with the private sector — in real-time.

The Workshop report summarizes recommended next steps in Section 2 and identifies best practices of leading supply chain organizations in Section 3.

Workshop Briefing Materials and Case Studies

Prior to the workshop, participants received executive-level briefing materials summarizing the results of seminal studies and articles on the new landscape of risk, with special sections on cyber risks, counterfeiting, new strategies for supply chain risk management, and U.S. and EU smart grid risk management strategies.

Additionally, best practice case studies from a number of companies, including Verizon, Dow, DuPont, Cisco, HP, and Telvent, highlighted industry approaches to supply chain security. A number of organizations provided tools and methodologies for supply chain security — both physical and cyber. These, along with the keynote presentations, can be found at www.usresilienceproject.org.

Section 2: Next Steps

Workshop participants saw an opportunity to expand the smart grid security lens beyond IT solutions and begin the process of engaging with the private sector to define a collaborative agenda for smart grid supply chain security.

There are two trends which make this topic ripe for dialogue. First, the growing convergence between physical and cyber risks creates an impetus to integrate IT and supply chain security into a holistic risk management solution for the smart grid. Second, building on business practices to narrow risks to the smart grid supply chain would enable the government to target its own resources to areas where the market drivers are insufficient, where the technologies to manage the problem do not exist or where the scope of threat is beyond the purview of companies or industries.

Workshop participants recommended a number of immediate next steps to accelerate adoption of best practices and strengthen public-private collaboration to secure the smart grid.

1. **Benchmark and Share Business Best Practice in Supply Chain Security and Resilience**
2. **Clarify Roles and Responsibilities in Public-Private Partnerships**
3. **Prioritize System Risks**
4. **Co-invest in Technologies**
5. **Foster Common Understanding of Challenges and Solutions**
6. **Leverage Synergies of Solution**
7. **Augment Professional Knowledge and Skills to Support Cybersecurity Solutions**

1. Benchmark and Share Business Best Practice in Supply Chain Security and Resilience

Workshop participants agreed that utilities and smart grid companies could learn from other sectors by benchmarking their best practices, processes, metrics and tools in supply chain risk management. These best practices need to be shared more broadly to help narrow the risks of counterfeit and compromised components in the smart grid.

DoE has extensive experience in working collaboratively with the private sector to secure the smart grid. Initiatives such as the National SCADA Test Bed, the consensus Roadmap to Achieve Energy Delivery System Cybersecurity, and the Electricity Subsector Cybersecurity Capability Maturity Model were built on the collective insights of owners and operators, commercial vendors, national laboratories, academia, industry associations and government agencies. These collaborative exercises created a collective plan to improve the security for smart grid IT systems.

Workshop participants proposed expanding the dialogue to include the supply chain cybersecurity and recommended that a future roadmap effort could:

- Benchmark best security practices in global supply chains and share experiences and practices with the power sector;
- Catalyze supplier summits to establish common expectations and requirements for supply chain security, integrity and continuity; and
- Create an ongoing interface for sharing supply chain information and mitigation practices between customers and suppliers.

2. Clarify Roles and Responsibilities in Public-Private Partnerships

Smart grid supply chain cybersecurity is a shared responsibility — with shared benefits. For government, securing the smart grid is essential to ensuring the growth, reliability and quality of the nation's power infrastructure. For companies, the security — both physical and cyber — of the supply chain is imperative to protect their brand, bottom line and shareholder value.

Benefits to both sides create a strong incentive to collaborate. One of the key pillars of effective partnerships is a willingness to define roles and responsibilities — not only by what must be done, but by which stakeholder has the best capability to do it. In many cases, the systems expertise, competencies and tools reside in the private sector. Companies need to commit to deploy commercial best practices, and government needs to integrate those practices in its cybersecurity planning and strategy for the smart grid.

Workshop participants recommended:

- Adopt private sector standards wherever possible;
- Recognize/reward best practice implementers;
- Expand information sharing, but go beyond threat information to sharing remediation and recovery best practices; and
- Enable non-attributed reporting from the sector to eliminate legal and regulatory concerns.

3. Prioritize System Risks

Supply chain risk managers typically develop a framework for prioritizing risks based on potential impact — and use that risk framework to set security requirements and allocate resources. For example, products or systems that come from areas deemed "high risk" warrant extra security precautions — boots on the ground and full track and trace capabilities, to name a few.

This kind of systems-based analysis will be essential for effective supply chain security for the smart grid. With potentially millions of devices on the system, it is neither feasible nor affordable to give every smart component in the supply chain the same level of physical and cyber scrutiny and security. Risks must be explicitly prioritized in order to develop a resource allocation strategy — with the most stringent requirements based on potential impact to the system.

Workshop participants recommended:

- Undertake systems level assessments to develop a risk prioritization framework, identifying the need for heightened security for technologies, components or systems where loss of performance or control could lead to national level impacts versus regional or localized impact.

4. Co-Invest in Technologies

One way to increase the security and resilience of the smart grid is to make the supply chain smarter — with track and trace technologies and sensor networks to enhance shipment security, intelligent packaging to thwart counterfeiting, anomaly detection tools, and analytic tools to identify geographic and vendor risks. The Workshop provided insights on additional opportunities to expand the collaborative technology agenda to smart grid supply chains.

Workshop participants recommended a number of high leverage opportunities for co-investment.

Technologies for risk assessment, including:

- Data analytics to assess risk holistically, automate risk assessment, identify anomalies and map supply chain tiers;
- Models to understand and prioritize system level risks; and
- Digital simulation of supply chain risks and resilience.

Technologies for supply chain cybersecurity, including:

- Detection of extra functionality in software or hardware;
- Capability to quarantine components;
- Techniques and testing systems to characterize and quantify risk; and
- Self-checking devices and systems, at the technical level.

Technologies for anti-counterfeiting, including:

- Intelligent, secure packaging (unique signature technology to distinguish genuine parts from counterfeit);
- Outbound beaconing; and
- Phone home capability to track locations of equipment and components.

5. Foster Common Understandings

There is a diversity of opinions — as large as the diversity of stakeholders — about what the supply chain cybersecurity problem is, who owns it, and what solutions are needed or available. Workshop participants suggested that a "Babelfish" capability was needed — a kind of universal translator that cuts across stakeholders, sectors and specialized languages.

The translation tools would clearly articulate the challenges and explain solutions in terms of the roles that individual stakeholders must play in their deployment. The goal is to encourage understanding and joint ownership of a solution set.

Workshop participants proposed several types of guidebooks to accelerate a common understanding of the risks and potential solutions:

- A guidebook for IT professionals to explain how supply chain best practices could help meet cybersecurity needs;
- A guidebook for utility supply chain professionals to showcase how best practices in supply chain risk and vendor management can help address the cybersecurity challenge;
- A guidebook for utility C-suites and boards on the need to connect information technology, operational technology, and supply chain in order to bring a holistic solution to smart grid cybersecurity — and how this can create cost efficiencies in security tools and processes;
- A guidebook for public utility commissioners on the convergence between physical and cyber security and the need to provide cost recoverability for end-to-end approaches that assure the reliability and integrity of the power infrastructure; and
- A guidebook for state and federal legislators to describe supply chain cybersecurity challenges, the need for end-to-end approaches and the need to build on existing business best practices for critical infrastructure security, rather than seek to regulate new ones.

6. Leverage Synergies of Solution

The use of cyber binoculars sometimes narrows the search for effective risk management tools. Tools, practices and processes that strengthen physical security and supply chain continuity can also help narrow cyber risks, but are often not seen as part of the cyber toolkit.

Good physical security at the manufacturing plant, in transit and in the warehouse can reduce counterfeit and cyber risks. By the same token, supply chain resilience programs can help secure the supply chain against counterfeit and compromised products in two key ways. In order to spot chokepoints and potential supplier continuity risks, resilience programs need to know who the vendors down the supply chain tiers are. This also creates a base of knowledge for creating a trusted vendor network. Resilience programs also create backup sourcing for key materials and components in the event of disruption. This also helps to reduce the risk that counterfeit or poor quality goods will enter the supply chain during crisis procurements.

These kinds of tools, which reside outside the IT security silo, have not typically been leveraged for cybersecurity but, of course, they could be. And, at the same time, they could increase the productivity and utility of existing investments in security and resilience.

Workshop participants recommended:

- Create key performance indicators (KPIs) for processes and capabilities;
- Create a web-based tool that communicates potential risks and issues across the corporation and provides for specific alerts that require a response; and
- Create mechanisms for communication among silos — engineering, legal, supply chain, quality assurance — to share lessons learned and best practices.

Examples of Synergies of Solution Among Supply Chain 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 and 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 vendor processes for quality assurance, 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

7. Augment Professional Knowledge and Skills

Managing the risk that compromised or counterfeit components could be inserted into the supply chain touches many professionals outside the IT function — site selection experts, manufacturing and quality assurance managers, procurement and logistics professionals, and anti-counterfeiting and supply chain security executives. In general, professionals outside IT functions receive very little training as to the nature of emerging cyber risks, or the role their best practices could play in reducing them. In many cases, they would benefit from better insights into the risks, a specific organizational role in cybersecurity strategy, and perhaps additional tools and skills to address cyber risks more effectively.

Workshop participants recommended:

- Include security and cybersecurity training and certification in professional disciplines, emphasizing that they have to be baked into every business process and operational function;
- Include professional development in supply chain security and cybersecurity as a positive element in personnel reviews and evaluation;
- Train regulators in business best practices in supply chain cybersecurity; and
- Assess needs for new skills, processes and tools to manage supply chain cybersecurity risks.

Section 3: Building on Business Best Practices to Secure the Smart Grid Supply Chain

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 will be a critical priority, and some of the best solutions are hiding in plain sight.

Participants at the workshop were asked to identify the best practices, processes and tools that their organizations were using to make their supply chains physically secure and resilient, and to protect the integrity of the products in the supply chain. They offered a number of operating principles, along with case study examples of how these principles are implemented. The four key areas of focus included:

1. **Organizational Best Practices**
   - 1a: Establish Risk Management Priorities
   - 1b: Manage Supply Chain Risks End-to-End
2. **Supply Chain Transparency and Trust**
   - 2a: Vet Supplier Practices
   - 2b: Build Trusted Networks
   - 2c: Deploy Information Systems and Analytics for Situational Awareness, Supply Chain Transparency and Resilience
3. **Supply Chain Security**
   - 3a: Establish Chain of Custody Controls
   - 3b: Deploy Anti-counterfeiting Controls
4. **Supply Chain Integrity**
   - 4a: Maintain Integrity of Electronic Components and Software throughout the Supply Chain

The following sections describe the specific practices and processes that companies have developed and deployed to accomplish these objectives.

1. Organizational Best Practices

1a: Establish Risk Management Priorities

Since it is impossible to protect every product against every contingency, the first step in risk management is a consequence analysis that helps to define potential impact. Risk managers need to understand potential consequences in order to determine whether the risk mandates a focus on prevention, mitigation or recovery. When a strategy becomes over-focused on prevention, workshop participants maintained that the challenge becomes infinite and the cost unaffordable.

Identified Best Practices Include:

- Develop a risk-based framework that prioritizes key components and technologies based on the potential impact for the business or the system.

BEST PRACTICES IN ACTION

Dow Chemical: Risk-Based Global Supply Chain Security Measures

Dow has developed a comprehensive risk management system for the safe and secure distribution of raw materials, intermediates and products worldwide. The system includes an assessment of potential safety and security risks across its chemical supply chain, including an evaluation of the safety and security practices of its raw material suppliers, the hazards of the materials shipped, the safety and security practices of its logistics service providers, the downstream uses of its products and the qualifications of customers to whom the products are shipped. This supply chain risk assessment and management program enables Dow to identify and implement appropriate, consistent, minimum safety and security measures for product, intermediate and raw material shipments worldwide.

Dow has prepared and implemented a supply chain security plan, which establishes a tiered system of risk-based security measures that increase with rising threat levels. Dow also has established transportation safety and security standards in those areas where additional risk reduction measures are desired above and beyond those required by government regulations. And, in those areas representing the greatest safety and security concern, Dow is pursuing industry-leading, state-of-the-art security initiatives.

DuPont: Finding the Right Balance Between Prevention, Mitigation and Recovery

From a prevention point of view, a company does as much as it can economically afford. Since it is impossible to protect against everything, the first step in risk management is a consequence analysis that helps define the potential impact. Risk management strategy requires knowing three things:

- What is the capacity to adapt?
- What are the mitigation plans (safe and secure shut down of the plant)?
- What capabilities are needed to respond and recover from events that may not have been anticipated and cannot be controlled?

1b: Manage Supply Chain Risk End-to-End

It would be hard to think of an activity that spans more functional specialties and stakeholders than supply chain. A "cybersecure" supply chain strategy begins in the design and development stage, and continues through manufacturing, shipping and warehousing, service and repair to end-of-life disposal. Cyber threats to the smart grid could emerge anywhere in that chain, and risks must be addressed holistically.

Identified Best Practices Include:

- Empower cross-functional teams for integrated supply chain risk management and incident response, including HR, legal, IT, security, finance and PR — and ensure that the team has decision-making authority.
- Create a web-based tool that communicates potential risks and issues (e.g. identification of counterfeit parts) across the corporation and provides for specific alerts that require a response.
- Create integrated workflow management processes — both automated and experiential — that provide overarching risk assessment from planning to training to response and feedback mechanisms. Capture learning from exercises and incidents with a focus on the human element.
- Perform constant benchmarking against other leaders in other sectors.
- Business continuity planning.
  - Expand business continuity councils to all internal stakeholders.
  - Practice and use business continuity plans, core failure models, drill and exercise continuously.
  - Require suppliers to have business continuity plans.
- Develop and deploy rapid response teams to plan and manage incident response. Create training exercises focused on supply chain issues, and involve suppliers.
- Develop a robust common language (terminology and problem definitions) to increase commonality in contracts and improve management of technology, products and processes.

BEST PRACTICES IN ACTION

DuPont: Integrating Supply Chain Efficiency and Effectiveness with Operational Excellence

The principles for supply chain efficiency and effectiveness are the same ones that guide operational excellence and productivity across the DuPont Production System. They are built on business integration, superior execution and centers for operational competency, which provide best practices, technologies and tools that are standardized and leveraged across DuPont's 13 businesses.

The goal is to create core processes that are simplified, standardized and sustainable. The supply chain operational centers of competency deploy practices and processes, technologies and models to drive continuous process improvement across regions and business platforms. In the supply chain area, the centers focus spans efficiency and risk management. It creates standards and processes to execute those standards — which are then deployed collaboratively with the business units.

DuPont Production System

Integrated Operations

Business Integration

- Strong supply chain integration within business teams and business strategies

Execution

- Drive effectiveness and efficiency in execution in plants and supply chains across businesses and regions

Operations Center of Competency

- Ensure organizational capability is in place
- Standardize and leverage

Deliverables

- Integrated strategies and operational plans
- Advancing core values
- Productivity and asset effectiveness among supply chains
- Capability building: people and organizational development
- Technology ownership and integration along supply chains
- Mindsets and behaviors that foster engagement and superior execution

BEST PRACTICES IN ACTION

Progress Energy: Linking Operational Technology, Information Technology and Supply Chain to Secure the Smart Grid

Business needs are driving requirements for increasing access and interoperability across enterprise applications, process computing environments, enterprise networks, and the Internet. Many times these business needs are in direct conflict with security objectives. To ensure communication and coordination, Progress developed a new Enterprise Architecture Review Process and created a committee made up of Operational Technology (OT) and Information Technology (IT) architects and engineers to provide standards, guidance and governance to 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. Collaboration between OT, IT and supply chain functions ensures that the right foundational capabilities (e.g. network security, authentication, monitoring, configuration management, etc.) are in the procured component or solution. The Supply Chain Operating Framework includes specific collaboration in the following areas: purchasing, contracting, category strategies (roadmap and strategy sharing), supplier management and performance monitoring.

2. Supply Chain Transparency and Trust

2a: Vet Supplier Practices

Global sourcing can create new risks at every link in the supply chain. New suppliers to the smart grid sector tend to have less understanding of customer requirements and may not meet quality or security expectations. In particular, the new hi-tech entrants into the smart grid supply chain do not understand the long technology life cycle of the power industry, which drives the need for more stringent security and performance requirements at the front end.

Even apart from the risk of malicious attacks on electronic components, the increased value of products flowing through the global supply chain has increased the incentives for cyber crime, counterfeiting and theft of digital IP. This has necessitated more organized processes to scrutinize suppliers in order to create confidence in the materials being sourced, the quality of the manufacturing process and the security practices of the vendors.

Identified Best Practices Include:

- Vet vendors as part of the RFP process through upfront security review and analysis.
- Gain visibility into who suppliers are — upstream and downstream.
  - Require vendor certification initially upstream and institute an ongoing vendor audit process, including site visits.
  - Use multiple sources to perform financial, legal and background checks on vendors to make sure they are qualified.
- Qualify supplier manufacturing processes and procedures.
- Tailor contract terms and conditions.
  - RFP requirements and contracts should be clear with respect to certification testing, vendor management controls, controls on where a product can be manufactured, quality controls and delivery practices — with a requirement for notification of any changes.
  - Contracts should specify requirements to protect intellectual property — to demonstrate a capability to compartmentalize and control information flow with verification provisions.
  - Implement detailed contract language to assess and verify supply chain risk, and oversee who is handling the product. Requires mapping of the supply chain and risk assessments of supplier companies.
  - Require timely notification by vendor in the event of a breach.
- Validate vendor supply chain security practices: real-time chain of custody controls with electronic verification, validation and authentication.
- Work with trusted vendors to assess, qualify and manage their suppliers.
- Impose robust and "boots-on-the-ground" audit processes.
- Ensure enhanced supplier awareness of best practices, including new ISO standards, training programs (PowerPoint, video), 1-800 number to call OEM or online access.

BEST PRACTICES IN ACTION

DOW: Risk Assessments of Raw Material Suppliers & Logistics Service Providers

Dow's suppliers are evaluated initially and periodically thereafter, based on the potential risks they present to the company. All suppliers are screened against specific criteria in eight risk areas, including safety and security, product stewardship, social and environmental responsibility, product quality, trade compliance, business continuity, financial stability and information protection. The criteria include attributes related to the supplier, industry sector, commodity, geographic area and markets served. All suppliers are ranked in one of three risk tiers: high, medium or low. Suppliers that are ranked in a medium or high-risk tier are further assessed using industry-developed protocols and internationally recognized certification standards, where available. Where industry protocols or government programs are not available, Dow-specific assessment protocols are used. Further, for suppliers ranked in a high-risk tier, Dow puts boots on the ground to validate that minimum risk management requirements are being implemented.

Schweitzer Engineering Laboratory (SEL): 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:

- Manufacturer location risk, based upon location for all process steps;
- Supplier quality risk, based on product 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's or supplier's financial health; and
- Purchasing risk, based on supplier performance for on time delivery and responsiveness.

Verizon: Processes for Vetting Vendor Practices

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, 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 control violations. 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 the 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 Ranking for Components and Suppliers:** Verizon prioritizes supplier 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 onsite reviews of high-priority vendors to ensure that they are complying with requirements and meeting appropriate security practices. Verizon employs onsite inspections and audits for these reviews, because there is concern that questionnaires may create a false sense of security. Vendors often give the answer that they think their customers want to hear or describe what the vendor believes is in place. Experience has shown that questionnaire answers rarely match up to the findings of onsite inspections.

2b: Build Trust in Supplier Networks

Best practice in supply chain processes is shifting from arms' length and sometimes adversarial relationships to collaborative networks to ensure quality and reliability, as well as product integrity. Trusted suppliers also understand customer expectations and needs.

While security technologies, contract clauses and more stringent standards are critical to securing the supply chain, a number of companies have found that face-to-face interaction with multiple tiers of suppliers is a best practice for communicating needs and expectations for quality, security and resilience.

Identified Best Practices Include:

- Share roadmap and strategy information with vendors and suppliers, challenging them to do the same with their suppliers, in an effort to communicate needs and expectations, as well as identify improvement opportunities to align product direction.
- Conduct annual supplier summits.

BEST PRACTICES IN ACTION

SEL: Building Trusted Supply Networks

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

- Share an overview of the company's history, values and corporate culture.
- Describe what its products do — and why lives depend on the quality and reliability of their products.
- Provide 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.
- 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.

HP: Solutions Across the Supply Chain

HP convenes an annual Suppliers Summit, bringing together more than 500 representatives from 150 suppliers, to share vision and priorities. The company 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.

2c: Deploy Information Systems for Situational Awareness, Supply Chain Transparency, Event Management and Resilience

Given the complexities of global infrastructure and interdependencies, it is impossible to accurately predict every possible risk trigger. Instead, global business leaders are creating new practices, processes, tools, technologies, metrics, and governance structures that rely on agility and adaptability. Resilience programs focus on putting in place the capabilities to manage a spectrum of disruptions, rather than specific scenarios. Information is the backbone of resilience — creating an ability to anticipate vulnerabilities, manage disruptions and recover rapidly.

Identified Best Practices Include:

- Map critical components to key hubs, nodes and suppliers to create situational awareness.
- Conduct annual assessment of supply chain risks: key sources, nodal vulnerabilities and single points of failure.
- Identify second and third tier suppliers, and assess financial health and business continuity plans.
- Deploy visualization tools/heat maps.
- Maintain a play book that enables deliberative rather than reactive responses.
- Validate supply chain continuity plans through audits and drills.

BEST PRACTICES IN ACTION

SEL: Creating Visibility to Evaluate Suppliers

SEL maintains a database of all the products it has manufactured — where they are coming from and where they go — to assure customers that the products are legitimate and have not been outside the SEL supply chain, and to be able to fast track efforts to ramp up production in the event of disruptions in the supply chain or demand spikes.

SEL also maintains a parts information database that covers every component. It collects data on supplier manufacturing locations; where materials are fabricated, packaged, tested, and shipped; and names of key people and contacts.

This data allows SEL 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 moved immediately 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 six months of inventory is continually secured for high-risk components, four months for medium risk, and three months for low risk.

SEL's Product Database collects information on:

- Product ID, firmware ID and serial number
- Subassembly data and work instructions
- Who built it?
- When was it 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 ACTION

Cisco: Supply Chain *Resiliency Index*

Cisco's business continuity program gathers a variety of information from its key supply chain partners through a survey process that occurs several times per year. The survey collects information on partners' business continuity practices (BCP), time to recover (TTR) in the event of a disruption and key emergency contact information, as well as financial information. With this data, Cisco can define the recovery profile of a product as characterized by the resilience of all component supplier factories, inventory hubs, partner production facilities and logistics centers within that product's value chain.

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, which is a key control point to assure the integrity of products in a globally outsourced supply chain. Each of these four elements of the *Resiliency Index* is in turn measured by an additional level of resiliency criteria. At the component level, for instance, the criteria includes the number of alternative sources of supply, component suppliers' TTR and end of life plans and processes. At the supplier level, resiliency is linked to the financial health of suppliers and partners, and suppliers' business continuity plans. Manufacturing resiliency is similar to component resiliency in that it is correlated with the availability of back-up or secondary sourcing and the manufacturers TTR following an event. Test resiliency is measured by the availability of inventories for long-lead test equipment parts. The *Resiliency Index* is applied automatically to Cisco's top 100 products that, in aggregate, account for about 50 percent of Cisco's revenue.

Information in Action

Within 12 hours of the initial Japanese earthquake in 2011, Cisco had identified all direct suppliers, their associated sites and components and other critical supply chain nodes in the impacted area. Leveraging the BCP contact information at the supplier level, the incident team was able to establish contact with suppliers to assess the impact on site capacity, and the prognosis of their ability to continue to produce and distribute components. Utilizing BCP Resilience Visualization capability, the team was able to develop a snapshot of the supplier impact and status over the entire region. In a short period, the crisis management system was able to assess more than 300 Tier 1 through Tier 5 suppliers, and more than 7,000 part numbers, and create a risk rating and mitigation plan. The largest supply chain disruption in modern times created virtually no revenue impact for the company.

Dow: Regional Event Management Centers

Within the last two years, Dow has created regional supply chain service event management centers to proactively monitor events that could adversely impact its global supply chain — from adverse weather conditions to anticipated labor disputes to social and political unrest to cargo theft and piracy — and manage those events to minimize any potential disruptions for customers. Covering the Americas, Asia, Europe/Middle East, Latin America and Africa, the regional centers draw on multiple intelligence streams to gather information and assess the potential impact of events on Dow shipments. For example, Dow's regional centers have managed potential disruptions associated with rail and port strikes in Europe and North America, typhoons in the South China Sea, hurricanes and tropical storms in the Gulf Coast, Houston ship channel closures due to a barge accident, political unrest in the Middle East, maritime piracy in the Gulf of Aden, and dangerous goods routing restrictions in China and other world areas associated with high-profile public events. The regional centers are building a strong library of lessons learned — i.e. what worked, what did not, and how the company could approach the problem differently in the future.

Once it becomes clear that an event could affect the company's product shipments or customers, the regional centers become the focus for risk management efforts. Depending on the potential severity of the event, the regional teams can put together a "war room" to monitor the situation, assess the potential impact, develop options and work directly with the affected business units, which in turn engage customers to determine ways to mitigate the impact of the disruption. The goal is to anticipate and adjust before a disruption can cascade into a major crisis for the company and its customers.

3. Supply Chain Security

3a: Secure Goods in Transit

Historically, the issues that caused the greatest impact on supply chains included natural disasters, severe weather, labor disputes and work stoppages, and social and political unrest. Globalization has dramatically expanded these risks, which now include terrorism and nation-sponsored attacks, pandemics, cargo theft, hazardous material accidents, product counterfeiting, smuggling and maritime piracy. The impetus to secure the physical supply chain has increased in importance.

Identified Best Practices in Physical Security include:

- Establish chain of custody controls that provide traceability and trackability using techniques such as:
  - Electronic validation to authenticate parts;
  - GPS tracking; and
  - Tamper detection techniques, including physical seals and sensors.

BEST PRACTICES IN ACTION

Dow Chemical Chain of Custody Controls

Dow's supply chain security is rooted in chain of custody controls. For highly valuable, highly regulated or highly hazardous 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 RFID tagging, 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 receives 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 container has been opened; whether the sensors detect light. There are shock detectors, which also 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 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:** catalyst materials and agriculture chemicals which could bring a high price on the black market;
- **High hazard:** materials that are toxic to inhale which could be used as weapons of mass effect by terrorists; and
- **Highly regulated:** chemicals that could be re-purposed 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.

3b: Deploy Anti-Counterfeiting Controls

Counterfeiting has grown dramatically — fourfold just during the last couple of years. With numerous high-profile examples of counterfeit parts undermining the integrity, functionality and longevity of critical systems, counterfeiting has come into the spotlight as a risk to customers, a cost to businesses (estimated at as much as $650 billion per year today and expected to double by 2015), and a threat to the integrity of critical infrastructures and defense systems.

Identified Best Practices Include:

- Institutionalize policies and procedures — clear direction on combating counterfeits or interdicting unwarranted functionality, and written guidance on how to avoid purchasing them.
- Buy only from OEMs and franchisees. Employ mitigation strategies if broker parts are purchased.
- Train on new threats, identification techniques and communications strategies.
- Employ packaging strategies including embedded security marking in parts; unique, harder-to-copy labels or markings; and distinctive lot and serial codes on external packaging.
- Deploy technological countermeasures, including:
  - Authentication or encryption codes.
  - Surface testing, X-ray analysis, electrical testing, thermal cycling, burn-in testing.
  - Embedded radio frequency identification in high-value parts.
- Destroy defective, damaged and retired parts.
- Institute inventory management controls on product returns and buy backs.
- Report occurrences of counterfeit goods both internally and externally.

BEST PRACTICES IN ACTION

SEL Product Integrity Assurance Program

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, every prospective procurement undergoes 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 they are out. All third party SEL suppliers work on a "one strike and you are out rule." If a third party source sends a counterfeit component, or components that 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.

SEL Policies

- Buy and sell direct, avoid brokers.
- Inspect packaging, track lot numbers.
- When in doubt, X-Ray, unpack and 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.

Dow: Most Effective Technology

Dow's Most Effective Technology (MET) Center provides solutions for a range of challenges, from anti-counterfeiting to supply chain safety and security.

One of Dow's emerging challenges is counterfeit products — either counterfeit Dow labels or real Dow labels with counterfeit product. For several high-risk businesses operating in high-risk geographies, Dow has implemented anti-counterfeiting approaches. For example, Dow places tamper-evident seals on containers to lower the probability of undetected entry. Second, the company has employed the use of holographs and 3D bar codes linked to a database of shipments, so distributors and customers can scan and verify the bar code through a link to Dow's secure database that the label is a legitimate Dow label and a legitimate Dow shipment.

HP's Counterfeiting Countermeasures

Counterfeiting is a significant concern for HP in an industry in which it is estimated that as many as 10 percent of products are counterfeit. HP is leveraging technology solutions, particularly in the printing and imaging areas, to reduce losses from counterfeiting and achieve a loss ratio that is well below the industry average. HP links printing innovation with Quick Response codes (QR codes) that can be used to check whether the product is genuine.

4. Maintain Integrity of Electronic Components and Software

Like the physical supply chain, the cyber supply chain is an end-to-end process beginning in the design and development phase and continuing through manufacturing testing, distribution, and service and maintenance. While physical security supply chain processes have matured, cybersecurity supply chain processes are still emerging. What became clear through this workshop is that physical and cybersecurity measures are complementary and need to be deployed together to create a trusted solution. The key in both areas is well understood and uniformly applied standards, practices and approaches across the global supply chain.

Identified Best Practices Include:

- Perform risk assessments on all new technologies and technology suppliers, and require third-party evaluation of significant new components.
- Adopt secure software development methodologies that make it harder to insert modifications.
- Verify and sign everything in design.
- Institute secure coding standards.
- Use cryptographic signing for hardware and software.
- Tailor contract requirements.
  - Include supplier QA standards and interoperability standards in contracts.
  - Clarify requirements for certification testing and vendor management controls.
  - Institute controls on where a product can be manufactured, quality controls and delivery practices — with a requirement for notification of any changes.
- Use stringent test protocols.
  - Include security testing of components as a standard, rather than random, testing procedures.
  - Deploy penetration testing to check attack vectors and develop internal databases to understand attack surfaces of products.
  - Institute third-party penetration testing of IT systems.
  - Conduct security, interoperability and functional tests before installation.
  - Institute ongoing testing, not just initial testing, with a focus on penetration testing.

BEST PRACTICES IN ACTION

Telvent: Secure Software Development

Telvent uses Agile software development, a methodology based on iterative and incremental development and collaboration between cross-functional teams. The Agile approach offers competitive advantages in terms of adaptive planning and flexible response to change, but it has some built-in security safeguards as well.

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 against vetted requirements by a Quality Assurance (QA) specialist assigned to the team. 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.

A second level of security is attained during the testing process. Every software development organization does testing. At Telvent, however, this is not a separate activity after the product development is complete. Testing is built into the development process from requirements validation to unit testing for each sprint to production testing for each software release. Once during each release cycle, each project team takes a one-day break in the coding cycle to stress test. This exercise, called "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: holes, places in the code with a single sign-on, hard-coded paths, legacy protocols, anything that creates or increases the threat surface. The rewards are geared toward finding and learning from mistakes, and there are prizes for those who find the most bugs and the most significant security threats.

Beyond human testing, Telvent uses machine-based automated testing scripts for highly complex scenario testing, as well as for regression testing. Automated testing is particularly valuable when used to evaluate the impact of newly released code on legacy applications. Machine-based testing can simulate multi-user conditions and highly repetitive tasks. While not specifically able to sniff for malware, automated test scripts can discover functional anomalies based on repetitive use conditions that can be base triggers for malware, such as Trojan horses or other kinds of disruptive functions.

Telvent: Secure Interoperability

Smart grid technology itself is often seen as a potential security problem because it opens utility grids to many potential penetration points, including the Internet. A smarter grid will require integration among systems that have traditionally been isolated, further extending the threat surface. But application of standardization and interoperability principles could increase the security of the smart grid. Standard architectural patterns and standard integration techniques make it possible to create great efficiencies, but also enable operators to identify anomalies more easily.

Telvent adheres to key architectural principles that enable the company to design in, rather than add on, security. By adopting a standard reference architecture, such as Microsoft's Smart Energy Reference Architecture, vendors can ensure that the integrated environment is built upon a foundation that has been designed with cybersecurity as a key requirement. Further, sticking to industry integration standards, such as the Common Information Model, allows for predictable integration with systems and devices beyond those delivered by a single vendor. Standard integration practices reduce customized code, a key failure point and a critical opportunity for cyber threat. Finally, solid architecture allows for the straightforward embedding of intrusion and malware detection and tamper-proofing tools that are built to provide internal security.

The most secure software products must eventually leave the development shop and be implemented in the real world of grid modernization. Implementation means that grid management software must touch and be touched by legacy systems and external devices with varying levels of security design and management tools. By adopting a standard architecture and using standard integration techniques, the threat surface from these external factors is significantly reduced.

Workshop Participants

Jon Amis
Supply Chain Risk Program
Manager, Dell

Sharla Artz
Director of Security/ Energy Policy
Schweitzer Engineering Laboratories

Jessica Ascough
Advanced Programs Engineer
Harris Corporation

Philip Auerswald
Associate Professor
George Mason University

David Batz
Manager, Cyber & Infrastructure
Security Edison Electric Institute

Ken Beichner
Vice President, Supply Chain
Elster Solutions

Adam Bishop
Manager, IT Security,
NRG Energy, Inc.

Jon Boyens
IT Specialist, Computer Security Division
National Institute of Standards and Technology

Christopher Boyer
Assistant Vice President for Public Policy
AT&T

Sandor Boyson
Research Professor & Co-Director, Supply Chain
Management Center Robert H. Smith School of Business
University of Maryland

James Brenton
Principal, Regional Security Coordinator
Electric Reliability Council of Texas

Stacy Bresler
Vice President, Outreach & Operations
EnergySec

James Briones
Project Manager, Energy Systems Security, NETL
U.S. Department of Energy

Larry Collins
Vice President E-Solutions
Zurich Financial Services

Edna Conway
Chief Security Strategist, Value Chain
Cisco Systems, Inc.

Joyce Corell
Director, Acquisition Risk Directorate
Office of the Director of National Intelligence

Vicki Cousino
Analyst, Acquisition Risk Directorate
Office of the Director of National Intelligence

Jeffery Dagle
Chief Electrical Engineer, Advanced Power & Energy Systems
Pacific Northwest National Laboratory

Michael David
Analyst, Acquisition Risk Directorate
Office of the Director of National Intelligence

Don Davidson
Chief, Outreach, Science & Standards
Trusted Mission Systems & Networks Office
U.S. Department of Defense

Paul Davis
Chief Technology Officer
NJVC

Ido Dubrawsky
Senior Principal Systems Engineer, Security Engineering
Team Lead Itron

Rhonda Dunfee
Control Systems Security
U.S. Department of Energy

Kevin Engfer
Director, Supplier Mission Assurance
Northrop Grumman Information Systems

Edward Erickson
Vice President
IntraPoint

Stuart Ferency
Chief, Critical Manufacturing Sector SSA
U.S. Department of Homeland Security

Gary Finco
Senior Advisory Engineer
Idaho National Laboratory

Michael Galluzzi
Supply Chain Manager
U.S. National Aeronautics and Space Administration

Josh Gerber
Lead Architect, Smart Grid
Sempra Energy

Bill Glynn
Director, Information Security
Westar Energy, Inc.

Edwin Goff
Enterprise Architect, IT&T Security
Progress Energy

Edward Gray
Vice President, Legislative & Regulatory Affairs
Elster Solutions

Carol Hawk
Program Manager, Cybersecurity for Energy Delivery
Systems U.S. Department of Energy

Darrell Highfill
Founder & Managing Partner
UtiliSec

Patricia Hoffman
Assistant Secretary
U.S. Department of Energy

Robert Hutchinson
Senior Manager, Information Sciences Group
Sandia National Laboratories

Rick Kahley Sr.
Category Manager, Meters and AMI Technology,
Exelon

Henry Kenchington
Deputy Assistant Secretary for Research & Development
U.S. Department of Energy

Himanshu Khurana
Acting Director for Global Technology, Knowledge Systems Laboratory
Honeywell

Kenneth Konigsmark
Senior Manager, Supply Chain & Aviation Security Compliance
Boeing

Theresa Lang
Director, Federal Security
Dell

Wayne Longcore
Chief Energy Solutions Expert
SAP

Troy Mattern
Military Executive Assistant to the Deputy Commander, U.S. Cyber Command
U.S. Department of Defense

Josh Magri
Associate Vice President
Internet Security Alliance

Reginald McCauley
Director, Supply Chain
Pepco Holdings, Inc.

James McConnell
Director of Security
Verizon

Jeffrey Meyers
Director of Smart Grid Sales
Telvent

Austin Montgomery
Smart Grid Program Lead
Software Engineering Institute,
Carnegie Mellon University

James Morozzi
President & Chief Executive Officer
GridWise Alliance

Nabil Nasr
Assistant Provost & Director
Golisano Institute of Sustainability
Rochester Institute of Technology

David Olive
Principal
Catalyst Partners

Mike Phillips
Corporate Information Security Director
CenterPoint Energy

Stacy Prowell
Chief Cyber Research Scientist Team Leader, Cyber Warfare Research Team
Oak Ridge National Laboratory

Kurt Ravenfeld
Director Strategy, Systems & Solutions, Global Supply Chain Operations,
Lockheed Martin

John Reynolds
Program Manager, SGSIA
McAfee

James Rice
Deputy Director, Center for Transportation & Logistics
Massachusetts Institute of Technology

Moses Schwartz
Member of Technical Staff, Cyber Analysis R&D Solutions
Sandia National Laboratories

Edmund Schweitzer
President & CEO
Schweitzer Engineering Laboratories

Shabbir Shamsuddin
Manager, Cyber Systems
Argonne National Laboratory

Henry Shiembob
Executive Director, Cybersecurity & Fraud Operations
Verizon

Frederick Smith
Director, GSG Programs & Supply Chain
Hewlett Packard

Robert Smola
Manager, Supply Chain Risk
Deere & Company

Rainer Sommer
Associate Professor, Public Policy and Enterprise Engineering
George Mason University

Charles Speicher, Jr.
National Director Smart Grid Major Opportunities & SGSIA
McAfee

James Steele
Program Director, Value Chain Risk Management, Global Business Operations
Cisco Systems

Roger Stough
Vice President for Research & Economic Development
George Mason University

Alfonso Valdes
Managing Director, Smart Grid Technologies
University of Illinois at Urbana-Champaign

Irvin Varkonyi
President
Supply Chain Operations Preparedness Education (SCOPE)

Larry Wagoner
Technical Advisor, NSA Cyber Task Force
U.S. National Security Agency

Guy Walsh
Domestic Partner Integration, Cyber Command
U.S. Department of Defense

Henry Ward
Global Supply Chain Director, Security, Sustainability & Public Policy
Dow Chemical

Chelsea White
Schneider National Chair of Transportation & Logistics
Georgia Tech University

Duminda Wijesekera
Associate Professor, Department of Computer Science
George Mason University

Donald Wirth
Vice President, Global Operations
Corporate Supply Chains
DuPont

Douglas Wylie
Manager Business Development, Networks & Security
Rockwell Automation

THE U.S. RESILIENCE PROJECT

Debra van Opstal
Executive Director

Dana Martin
Deputy Director

Denise Swink
Senior Advisor

William Booher
Senior Advisor

Shannon Hayes
Special Assistant

ENERGETICS INCORPORATED

Katie Jereza
Program Director & Breakout Facilitator

Howard Andres
Breakout Facilitator

Fred Hansen
Breakout Facilitator

Brian Marchionini
Breakout Facilitator

Rebecca Massello
Breakout Facilitator

Melanie Seader
Breakout Facilitator

Samantha Solomon
Breakout Facilitator

Gareth Williams
Breakout Facilitator

OBSERVERS

Hasan Aijaz
Research Associate, Center for Infrastructure Protection & Homeland Security George Mason University

Nobuhiko Daito
Doctoral Student
George Mason University

Zhenhua Chen
Doctoral Student
George Mason University

Sachin Garg
Doctoral Student
George Mason University

Workshop Agenda

7:30 COFFEE AND PASTRIES

8:30 WELCOME

Roger Stough
Vice President, Research, George Mason University

Debra van Opstal
Executive Director, U.S. Resilience Project

8:45 GOALS FOR THE WORKSHOP

Patricia Hoffman
Assistant Secretary for Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy

9:00 FRAMING THE ISSUES: KEYNOTES

Ed Schweitzer
CEO, Schweitzer Engineering Laboratory

Ed Goff
Enterprise Architect IT&T Security, Progress Energy

9:45 FRAMING THE THREAT ENVIRONMENT

Robert Hutchinson
Senior Manager for Computer Science and Information Operations, Sandia National Laboratories

10:00 SETTING THE STAGE FOR BREAKOUTS

Key Observations and Findings

Debra van Opstal
Executive Director, U.S. Resilience Project

Denise Swink
Senior Advisor, U.S. Resilience Project

Risk Framework

Edna Conway
Chief Security Strategist, Value Chain, Cisco

Breakout Group Logistics

Katie Jereza
Program Director, Energetics Incorporated

10:30 NETWORKING BREAK

11:00 BREAKOUT SESSIONS

Managing Supply Chain Cyberrisks: Building from Business Best Practice

Participants in the workshop will break into four groups to explore best practices to prevent, detect or mitigate: malicious substitution of hardware or software via the supply chain; substitution of counterfeit products/tampering in the supply chain; misuse of IP by supply chain partners; degradation of security protocols in crisis situations. The groups will also address gaps in protection and opportunities for collaborative solutions, technologies and smart policy. Working lunch provided.

2:00 NETWORKING BREAK

2:30 REPORT OF FINDINGS AND RECOMMENDATIONS FROM BREAKOUT LEADERS

3:45 NEXT STEPS

Hank Kenchington
Deputy Assistant Secretary for R&D Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy

4:00 ADJOURN

About the U.S. Resilience Project

Building on Business Best Practices to Meet National Challenges

The primary goal of the U.S. Resilience Project (USRP) is to advance cutting-edge resilience policies, practices, and public-private partnerships by:

- Capturing cross-sector business best practices, processes and tools for resilience and preparedness;
- Creating a framework for public-private partnerships that builds on key competencies and best practices; and
- Educating public and private sector executives in cutting-edge tools and management strategies.

Key Concepts

Warning: Turbulence Ahead. The one thing we know with certainty is that the future will be volatile and uncertain.

Capturing the Business Case for Resilience. Since it is impossible to accurately predict every possible risk trigger, business leaders are creating new strategies that rely on agility and adaptability

Building Best Practices into National Strategies. Existing best practices in enterprise resilience already go a long way toward serving national mission needs, but are not always integrated into government strategies.

Valuing the 75 Percent Solution. Although government and industry objectives are not identical, private sector best practices can contribute significantly to national resilience — and free up government resources to address gaps.

Creating Two-way Partnerships. Partnerships must be built around defining key roles and responsibilities, based on capabilities, competencies and mission objectives.

Expertise

Debra van Opstal, executive director of the USRP, was formerly a senior vice president at the Council on Competitiveness, authoring *Transform: The Resilient Economy*.

Henry Ward, a Distinguished Fellow at the USRP, recently retired as the Global Supply Chain Director of Security, Sustainability and Public Policy for Dow Chemical.

Denise Swink, a senior advisor of the USRP, has more than 35 years of experience in management and supervisory positions, with key expertise in public-private partnerships, manufacturing, and infrastructure interdependencies.

William Booher, a senior advisor of the USRP, was formerly executive vice president and treasurer of the Council on Competitiveness.

Steve Shiffer, a senior advisor to the USRP, is an expert in supply chain risk management and lean enterprise.

Alison Walsh produces the USRP publications and reports. Ms. Walsh is a freelance consultant with more than 10 years of experience writing, editing and creating publications for a broad range of industries.