2012 DOE Smart Grid Cybersecurity Information Exchange

December 5-6, 2012 • Washington, D.C.

TABLE OF CONTENTS

Executive Summary

Recipients of the American Recovery and Reinvestment Act of 2009 (ARRA) Smart Grid Investment Grants (SGIG) and Smart Grid Demonstration Program (SGDP) are in the midst of installing nearly $8 billion in advanced smart grid technologies and systems that could dramatically change the way electricity is produced, managed, and used in the United States. One of the key challenges for utilities is to implement smart grid devices and systems while ensuring and enhancing the cybersecurity of these digital systems. Toward this end, the *2012 DOE Smart Grid Cybersecurity Information Exchange (2012 Information Exchange*) held in Washington, DC on December 5 and 6, 2012, enabled SGIG and SGDP recipients to: (1) share information and lessons learned in developing and implementing their Cybersecurity Plans (CSP); (2) learn about available tools, techniques, and resources for strengthening the security of cyber systems; and (3) gain a common understanding of how to sustain cybersecurity processes once the ARRA projects are completed.

Through interactive peer-to-peer exchanges, panel discussions, expert presentations, and poster sessions, attendees of the *2012 Information Exchange* discussed critical issues and insights arising from the implementation of their cybersecurity programs and looked to the future of cybersecurity for the electric grid. These discussions produced important lessons learned and best practices from implementing cybersecurity in smart grid systems. They are summarized below:

1. *Lessons Learned and Best Practices from Site Visits*
   - Learn from other utility cybersecurity deployments
   - Planning is key for successful CSP implantation
   - Defining ownership and roles is necessary
   - Strive to stay ahead of the trends
   - Obtain management support
   - Seek to actively engage and inform the customer
2. *Technology Gaps and Dealing with the Pace of Change*
   - Enact standards and clarify language
   - Planning and scaling for future cybersecurity technologies is key
   - Ensure interoperability and testing/certification
3. *Value Proposition For The Cybersecurity Plan Beyond ARRA*
   - The CSP is valuable as an educational tool
   - The CSP helps to allocate scarce resources
   - The CSP provides a mechanism for cybersecurity planning

- The CSP facilitates dialogue among cybersecurity stakeholders
- Cybersecurity must become company culture

4. *The CSP Should Act Like A Business Plan*
    - Need to explain the opportunity cost of not undertaking cybersecurity
    - The CSP details risk management
    - The CSP prioritizes project funding
5. *Working with Vendors*
    - Vendors need to track asset through end-of-life
    - Flexibility and persistence pays off when working with multiple partners
    - Device design should focus around functionality and security
    - Build a common understanding
6. *Lessons Learned for DOE*
    - DOE onsite cybersecurity visits are beneficial to recipients
    - DOE has a role in future cybersecurity efforts coordinating and facilitating information
    - DOE should play a role in setting standards

Attendees identified the continuing issues and needs in implementing successful cybersecurity programs. These are summarized below:

1. *Integration of Cybersecurity Programs*
    - Budget
    - Corporate culture
    - Workforce training
    - Privacy concerns
2. *Technology Gaps and Dealing with the Pace of Change*
    - Procurement
    - Device standards
    - Open access to system networks
    - Life cycle
3. *Working with Vendors*
    - Vendor expertise
    - Working with multiple partners
    - Features and services
4. *Adapting Your Company to Create a "Culture of Cybersecurity"*
    - Creating a culture of cyber security
    - Changing perspectives
    - Identifying the "right" person at the "right" time
5. *Challenges of CSP Significance*
    - Lack of management "buy-in"
    - Issues with company resources
    - CSPs are viewed as static and not maintained as defining a living process

DOE-OE uses the *Cybersecurity Information Exchanges* as a critical tool to gain direct feedback from the private sector on its smart grid cybersecurity needs, and uses this input to identify needed tools and technologies, shape programs, and direct resources. The valuable best practices and lessons learned that were captured will become essential components of DOE-OE's future smart grid outreach. Participants are strongly encouraged to share their successes with peers, strengthen connections built at the workshop, and continue engaging DOE-OE on remaining needs.

BACKGROUND

In 2010 and 2011, recipients of the American Recovery and Reinvestment Act of 2009 (ARRA) Smart Grid Investment Grants (SGIG) and Smart Grid Demonstration Program (SGDP) began installing advanced digital devices for the smart grid infrastructure. Many projects which already had cybersecurity plans (CSPs) refined and implemented their CSPs to meet award requirements.

The U.S. Department of Energy Office of Electricity Delivery and Energy Reliability (DOE OE) hosted the *2011 DOE Smart Grid Cybersecurity Information Exchange* (*2011 Information Exchange*) in Chicago, Illinois in August 2011 as a peer-to-peer exchange to learn and better understand what was required in the CSPs and to impart lessons learned from annual site visits.

In July 2012, DOE OE published the *SGIG Progress Report* which reported on the progress made by SGIG recipients in installing smart grid tools and systems.

The *SGIG Progress Report* reported that:

- DOE required all recipients to develop cybersecurity plans that provided information about how they would identify cybersecurity risk, how those risks would be mitigated, and how the processes in place would ensure that a sufficient cybersecurity posture be maintained.
- DOE OE created a dedicated and secure website to help SGIG recipients manage their CSPs and promote sound cybersecurity policies and practices. The website provides information, tools, and resources from government and industry sources.

- DOE OE hosted two cybersecurity webinars for SGIG recipients. The first webinar, conducted in January 2010, reiterated the SGIG cybersecurity mission and reviewed requirements for the CSPs. The second webinar, conducted in February 2011, assisted recipients develop an effective response to smart grid cybersecurity requirements.
- In 2012, DOE OE conducted site visits to ensure that each SGIG recipient was implementing cybersecurity methods and approaches consistent with their CSP.

The *2012 DOE Smart Grid Cybersecurity Information Exchange (2012 Information Exchange)* was held in Washington, DC on December 5 and 6, 2012.

The *2012 Information Exchange* enabled SGIG and SGDP recipients to: (1) share information, best practices and lessons learned in developing and implementing their CSP; (2) learn about available tools, techniques, and resources for strengthening the security of cyber systems; and (3) gain a common understanding of how to sustain cybersecurity processes once the ARRA projects are completed.

Best Practices and Lessons Learned

The breakout sessions were devoted exclusively to information exchange among grant recipients. Facilitated breakout groups allowed recipients to share best practices from their project experience, lessons learned that can apply to other grant recipients and other utilities, and remaining challenges and issues in implementing cybersecurity solutions in five technology areas (See Agenda for a list of the breakout topics). Below is an outline of the major lessons learned and best practices that were identified and discussed during the *2012 Information Exchange.*

Lessons Learned and Best Practices from the 2012 Site Visits

In 2012, DOE OE conducted site visits to ensure that each SGIG recipient was implementing cybersecurity methods and approaches consistent with their CSP. The recipients shared key cybersecurity insights gained during the 2012 SGIG site visits. Actively sharing lessons learned from the DOE OE-guided site visits becomes especially important as the SGIG and SGDP projects move into their final stages. These best practices and lessons learned will help to inform future cybersecurity investment and implementation decisions made by the recipients. Comments are captured below in Table 1.

Table 1: Site Visits Lessons Learned/Best Practices

Best Practice or Lesson Learned	Comments
Learn from other Utility Cybersecurity Deployments	• Utilities find it beneficial to conduct and share assessing, identifying, and mitigating risks at each stage of the development lifecycle. • Taking the time for lessons learned during the pilot before full production and rollout can help ease transition to the implementation phase. • Adherence to relevant cybersecurity standards and/or best practices provides a smoother implementation path.

Best Practice or Lesson Learned	Comments
Planning is Key	• Development of cybersecurity specific procurement contract language when procuring systems, products and related services can prevent future issues from arising. • Establish a secure, compliant, trusted communication channel/ repository early to facilitate the exchange of sensitive information. • Consider early engagement of 3rd party software suppliers to gain access to documentations, details, etc. • To the extent possible, systems must have upgrade capability to meet future requirements but also strive for simplicity. • Assess the impact of cybersecurity measures on other critical grid control functions.
Defining Ownership and Roles is Necessary	• Defining VPN connections to ensure that one entity owns and manages both endpoints of the VPN tunnel to simplify troubleshooting and maintenance is essential. • Maintain an organizational chain of accountability to senior management. • Create a cybersecurity/assessment plan detailing roles and responsibilities of each party. • The security team should be involved throughout the process, not after the fact. The team should meet in–house before awarding contracts; planning and training is critical to success.
Strive to Stay Ahead of the Trends	• Support emerging smart grid cybersecurity standards. • Consider interoperability, not just device security. • Learn from utilities' experiences with trends in technologies and their implementation. • Become active in national groups to share information.
Obtain Management Support	• Support for cybersecurity programs must come from the top down to ensure the cybersecurity program is successful. • Obtain upfront management support and keep executives informed throughout the project. Explain the business benefits of each maturity level and let the executives decide.
Seek to Actively Engage and Inform the Customer	• Communication to the customer must be a priority (e.g., contract, bill of rights, security communication, benefits to customers). • There is a need to specify and communicate what data is being collected and why collecting it can alleviate customer concerns. • Utilities need to correct misinformation and provide accurate privacy information to consumers. • Utilities should treat usage data as Personally Identifiable Information (PII). • Utilities can undertake educational campaigns for customers. o Public perception of utilities can be improved through education and more effective communication with customers.

Technology Gaps and Dealing with the Pace of Change

Current technologies and products offered may not meet all cybersecurity requirements outlined in utilities' CSPs. Attendees identified gaps in technologies, products, processes, and information that would enable utilities to improve their cybersecurity posture. The recipients shared best practices and lessons for overcoming these gaps in the process of installing cybersecurity technology tools and devices. Comments are outlined below in Table 2.

Table 2: Technology Gaps and Dealing with the Pace of Change

Best Practice or Lesson Learned	Comments
Enact Standards and Clarify Language	• Demand that standards are used in all products rather than the use of proprietary technology. • Negotiate standards with vendors beforehand so they know where they need to start. • Utilities should contractually address security concerns. • Provide strong contractual language in Request for Proposals (RFPs). o Consider what happens in a zero-day situation. o Send letter to vendors with procurement requirements as well as in RFPs.
Planning and Scaling for Future Cybersecurity Technologies is Key	• Writing CSPs for new classes of devices not yet in production is challenging. o Build flexibility into projects and monitor them. o Make decisions and act on them to get technology implemented. o Do not let "better" get in the way of "good enough." • Perform R&D on scalable key components. o Develop database of discrete components, though this can be difficult to maintain with thousands of components. o Develop technology that is more upgradeable without having to upgrade the modules.
Ensure Interoperability and Testing/Certification	• Collaborate with manufacturers for more robust testing. • Create interoperability with legacy systems through gateway proxies and service buses. • Create test environments that are fully representative of all factors in the field. o This can be difficult for utilities; perhaps leverage industry capability. • Communicate what the certification actually means. • Create a certification process (Institute of Electrical and Electronics Engineers [IEEE] checklist for hardware, software, and cybersecurity or something similar).
Develop Methodology for "Failing Securely"	• Create a risk management framework. o Set up models for every use to develop methodologies to respond to each unique fail-secure issue. o Build mechanisms into new systems that mitigate risk. o Allow the ability to mirror systems or run systems in parallel. o Promote resilience during an attack/emergency. o Use network detectors for when breakers open and close. o Create authentication mechanisms for passwords.

Value Proposition for the Cybersecurity Plan beyond ARRA

Every SGIG and SGDP project was required to develop, implement, refine, and manage a comprehensive CSP. As SGIG and SGDP projects are completed, utilities must decide how they will maintain a strong cybersecurity posture for their smart grid systems and to what extent CSPs will contribute. Attendees identified where plans have been effective and how they can be adapted to contribute to post-ARRA funded cybersecurity projects. Comments are outlined below in Table 3.

Table3: Value Proposition of CSP Beyond ARRA

Best Practice or Lesson Learned	Comments
The CSP as an Educational Tool	• The CSP has facilitated communication of cyber standards and guidelines within companies and across sectors. • There was not much experience previously on developing cybersecurity plans, so this requirement created a general education.
The CSP Helps to Allocate Scarce Resources	• The CSP has helped to develop and/or justify budget requests and personnel hiring. • The CSP has provided justification for security liaison roles (funded positions in both IT and OT for nexus points to drive posture forward). • The CSP provides adequate allocation of resources across the organization.
The CSP as a Mechanism for Cybersecurity Planning	• The CSP has helped apply the appropriate licensing. • The CSP has lead to increased critical infrastructure protection. • Helps recipients plan to use their CSPs as a mechanism to meet safe public service requirements. • The CSP should be used as a foundation for post-ARRA cyber work, but recipients should adapt it to meet future projects and needs. • The CSP provided an impetus to adapt broader standards (i.e., not focused just on security).
The CSP Facilitates Dialogue	• The CSP has allowed utilities to open up dialogues with organizations in which they have never collaborated with previously. • Helps recipients plan to continue dialogue with transmission owners and operators.
Cybersecurity must become Company Culture	• Companies need to undertake culture change. o The CSP drives best practices and sharing of lessons learned. o The CSP helped to streamline regulatory structure, or at least work out incompatibilities. o The CSP helped to develop a common vocabulary, which is important. • Security as a culture involves creating security liaisons for Operations Technology (OT) and Information Technology (IT) Divisions. • Merging IT and OT so that each group recognizes the validity of each others' concerns and priorities is a result. • It is important to have all involved understand various IT and security requirements. o Cybersecurity risk mitigation prioritization, evaluation and implementation must involve senior management, along with functional and business managers. • Make CSPs living documents that can be adapted to project needs.

The CSP Should Act like a Business Plan

Managing cyber risks often presents a much greater challenge for the utilities compared to managing physical risks. Security directors often struggle to quantify and communicate the importance of cybersecurity issues to their managers and CEOs, and funds may not be available for cybersecurity investment unless it is directly related to compliance. All this contributes to a persistent problem: how to build the business case for cybersecurity. Attendees identified solutions to selling the business case on cybersecurity. Comments are outlined below in Table 4.

Table 4: Imitating the Business Plan

Best Practice or Lesson Learned	Comments
Explain the Opportunity Cost of Not Undertaking Cybersecurity	• A CSP should behave like a business plan that includes a budget, defined risk, metrics and evidence and is written so that senior management can understand it. • Show senior management what the mitigation opportunity is by demonstrating consequences of an intrusion. • Tie security needs to the businesses strategy. • Create quantifiable metrics that can be applied to security.
The CSP Details Risk Management	• Management worries about risk, revenue and delivery. Successful communication shows the risk, and getting management to address or accept that risk. • Cybersecurity is not only insurance. Articulate the business case as an operational requirement. • Show management how investment in security can reduce risk.
The CSP Prioritizes Project Funding	• How to prioritize needs in the future is critical to future success. • The CSP as a “business plan” helps decide if it necessary to do a further project or to continue funding the current project post-ARRA.

Working with Vendors

SGIG and SGDP grant recipients are in a unique position to share their experiences working with vendors. Because technology changes occur rapidly, it is important that the industry as a whole learn from those who have had both good and bad technology and vendor relationship history to share. Participants discussed their best practices and lessons learned with working with outside vendors. Major points on the topic are summarized in Table 5 below.

Table 5: Working with Vendors

Best Practice or Lesson Learned	Comments
Vendors Need to Track End of Life	• Vendors need to take responsibility for lifecycle of their products to ensure that devices are adaptable. • Get vendors to track commercial, off-the-shelf technologies used in their products. o Vendors should notify asset owners after the end of life.
Flexibility and Persistence Pays Off when Working with Multiple Partners	• In collaborating with multiple partners: o Be persistent in dealing with multiple organizations. o Have an open dialogue, maintain regular meetings, or call in a third party to facilitate/negotiate. o Have flexibility in creating plans that cover all organizations or each one individually. • Utilities can collaborate with consultants (particularly with smaller organizations), at workshops and with user groups. • Utilities should look to collaborate with partners they traditionally have not worked with before.
Device Design	• Vendors need to focus on functionality and also security. • Vendors are starting to make products more user- friendly. • Specify up-to-date security in procurement documents. • Create a "Vulnerability Disclosure" where the vendor is required to disclose requirements.
Build a Common Understanding	• Negotiate standards with vendors beforehand so they know where they need to start. • Communicate with all the stakeholders (utilities, vendors/providers, customers) the issues for rollouts. • Undertake vetting and relationship building with vendor so that they understand the utility's service territory. • Work with the vendors to determine testing activities. • The more utilities that require advanced security, the more responsive the vendors will become- this will be critical to determining the success or failure of a product.

Lessons Learned for DOE

As SGIG and SGDP project recipients refine and implement their CSPs they are learning what works, what does not work, and what critical challenges could arise along the way. During the *2012 Information Exchange,* the recipients shared best practices and lessons that could be applied to future DOE OE smart grid programs. Major points on the topic are summarized in Table 6 below.

Table 6: DOE Lessons Learned

Best Practice or Lesson Learned	Comments
DOE Onsite Cybersecurity Visits are Beneficial	• In the future, DOE OE should continue its onsite review as it often provides the utility with incentives to move forward with requirements defined in their CSPs and to learn from DOE cyber experts.
DOE has a Role in Future Cybersecurity Efforts	• DOE should share more peer-to-peer information on cybersecurity by convening future work groups. • DOE should continue to develop and maintain the cybersecurity questions over time to ensure questions remain relevant. • DOE should consider providing training to help utilities use the DOE Electricity Subsector Cybersecurity Capability Maturity Model (Maturity Model). • DOE should collect best practices to share with the industry and not just the SGIG and SGDP program participants. • DOE can help tell the story by relating why enacting cybersecurity programs are critical from a reliability standpoint or from a customer standpoint. • DOE should continue its current effort coordinating with industry to update U.S. Department of Homeland Security procurement language. o DOE should post on its website cyber boilerplate language.
DOE Should Play a Role in Setting Standards	• DOE should develop some accepted standards or a ”seal of approval.” o A DOE guidance manual for the Maturity Model is needed. o DOE guidance can include recommendations on how to use the Maturity Model for planning purposes.

SGIG/SGDP Cybersecurity Issues and Needs

Below is an outline of the major needs and gaps that were identified and discussed during the *2012 Information Exchange.* This summary of issues is based on presentations, questions and answers and discussions from breakout sessions.

Integration of Cybersecurity Programs

For some SGIG and SGDP recipients, planning and budgeting for cybersecurity programming is a new process. The ARRA-funded grant requirement to establish a CSP has been the driver for many of the recipients to establish cybersecurity programs. Challenges have arisen in formulating cybersecurity budget planning and processes. Some of the major issues on how to successfully integrate a robust cybersecurity program are included the points in Table 1 below.

Table 1: Integration of Cybersecurity Programs

Issue	Comments
Budget	• Budgets need to be developed and supported by all levels within the company. • Inaccurate interpretation and/or misunderstanding of policies and/or guidelines results in delays and cost issues. • The industry is still developing cyber expertise and needs resources to hire and retain cyber personnel.
Corporate Culture	• Incompatible expectations or timelines make it difficult to create and implement successful cybersecurity programs. • Undefined personnel roles and responsibilities are major obstacles and must be established at the beginning of any cybersecurity program. • Company "silos" need to be overcome so the cybersecurity program is well understood by all. • The need for an enterprise-wide cultural change often exists. • The gulf between operations and IT staff needs to be narrowed.
Workforce Training	• Gaps in training technical staff are a major obstacle to success. • Cyber staff needs to develop skill sets to be able to articulate program requirements to executives.
Privacy Concerns	• Privacy concerns both for the consumer and the utility are of major importance. • Customers want to see data, but utilities have concerns about exposing data due to security issues.

Technology Gaps and Dealing with the Pace of Change

Implementing cybersecurity systems often requires the installation of new products and tools. Technology development is evolving rapidly. The ability to undertake critical analysis of what is the appropriate level of investment in cybersecurity technology is daunting. Attendees discussed the many challenges to the installation of cybersecurity technology tools and devices. Comments are outlined below in Table 2.

Table 2: Technology Gaps and Change

Issue	Comments
Procurement	• Writing cybersecurity plans for new classes of devices not yet in production is extremely challenging. • There is a lack of code review or certification standards to use. • Procurement language does not help with early adopter costs. • Nature of existing procurement language does not allow flexibility to the customer. • New requirements for cybersecurity systems planning are difficult without a company history. o Geographic constraints make procurement difficult in both physical distance and wide-area networks. • Sparse distribution of technologies in the field is a challenge. • While the DOE OE Maturity Model provides a clear roadmap, it does not provide direction to utilities on how to address the issues and enact change.
Device Standards	• Wireless devices are not always configured as advertised by vendors. • Alarms are not standardized and can be confusing across multiple vendors. • Devices either do not have passwords, the passwords are all the same, or the passwords are managed in a spreadsheet.
Open Access	• Utilities are doing controls from trucks and mobile devices (iPads). • Lines for communication with devices on poles are completely open. • Access to communications from a field device is not considered adequately. • Encryption is not used in communication path. • Meter encryption is shut off for almost any issue. • Issues exist with developing metrics for interfacing syncrophasor architectures in end-to-end environments. • Remote access for vendors and support is not properly secured. • Third party communication suppliers do not secure to utility satisfaction.

Issue	Comments
Life Cycle	• Dealing with beyond end-of-life issues ("sunsetting" of devices) is difficult. • Triage concerns exist in a resource-constrained environment. • Vendor support for old devices is usually impossible. • Product immaturity – vendors are figuring it out as they go. o Synchrophasor technology is still evolving, so it is difficult to maintain CSPs for projects installing these devices. • The lifecycle of devices changes too rapidly.
Testing	• Need credible entity to normalize consistent testing. • Gaps exist in testing and certification. • Need to have accreditation authority identified. • Testing scalability of systems needed.

Working with Vendors

Utilities must rely on and work closely with vendors of cybersecurity technologies and systems. This reliance on outside partners often proves to be challenging as trusting relationships take time to develop, products needs to be customized, and technology is evolving rapidly. Participants discussed their experiences with working with outside vendors. Major points on the topic are summarized in Table 3 below.

Table 3: Working with Vendors

Issue	Comments
Vendor Expertise	• Utilities need to update procurement language so that it can be put in a letter to vendors in advance before RFP comes out. • Many vendors do not understand specific security requirements and standards have not often been defined during the procurement process. • Vendors may have their own ideas about appropriate protocols, which may not be current. • Third party security products are problematic. • Security solution may not live up to advertised capability. • Smaller utilities must rely on vendor expertise.
Working with Multiple Partners	• Multiple participants are needed to coordinate CSPs to cover DOE requirements. • Multiple distribution partners have different equipment and policies regarding data security. • Collaboration sometimes is not possible due to reticence about competition. • Cost is a factor when dealing with multiple partners.

	• Vendor silos make it difficult for projects.
Features and Services	• New vendor features and services are proprietary and confusing and are not consistent among vendors. • Vendors do not want to go back and do R&D after delivering a product that does not address all the requirements. • Interoperability among vendors and lack of standards impact security because encryption might be proprietary, and the software or device is incompatible. • Standards are still being developed.

Adapting Your Company to Create a "Culture of Cybersecurity"

The modernization of the U.S. electric grid has enabled the emergence of new cybersecurity technologies and mitigation techniques. Utilities must train their employees to not only implement new technologies but also teach operational and informational technology divisions to work together to implement cybersecurity for the smart grid across the enterprise. This new system-wide collaboration involves creating a "culture of cybersecurity" within all aspects of the utility. Participants discussed their experiences with working to make a "culture of cybersecurity" within their company. Major points on the topic are summarized in Table 4 below.

Table 4: Adapting Your Company

Issue	Comments
Creating a Culture of Cyber Security	• There is a lack of common vocabulary on cybersecurity issues. • There is a need for enterprise-wide cultural change. • There are gaps for training technical staff including general employee awareness or executive level involvement. • General lack of training across the industry exists, with the need to develop the right skill sets. Across a company there are inaccurate interpretations of cybersecurity policies and/or guidelines. • The gulf between operation and IT staff requirements needs to be narrowed.
Changing Perspectives	• Understanding differences in departmental perspectives is critical. • Within the same organization there are different cultures to be aligned, and each company must determine how to work together and when "enough is enough." • Core elements of cybersecurity work are in competition for the same funds as other parts of the company.
Identifying the "Right" Person at	• Getting the right people together and coming to an understanding is imperative. o It is challenging to implement smart grid projects when a number of stakeholders are involved.

the “Right” Time	• Utilities are often stove piped, so there is also often no corporate-wide security plan. • Hiring and retaining cyber experts is challenging.

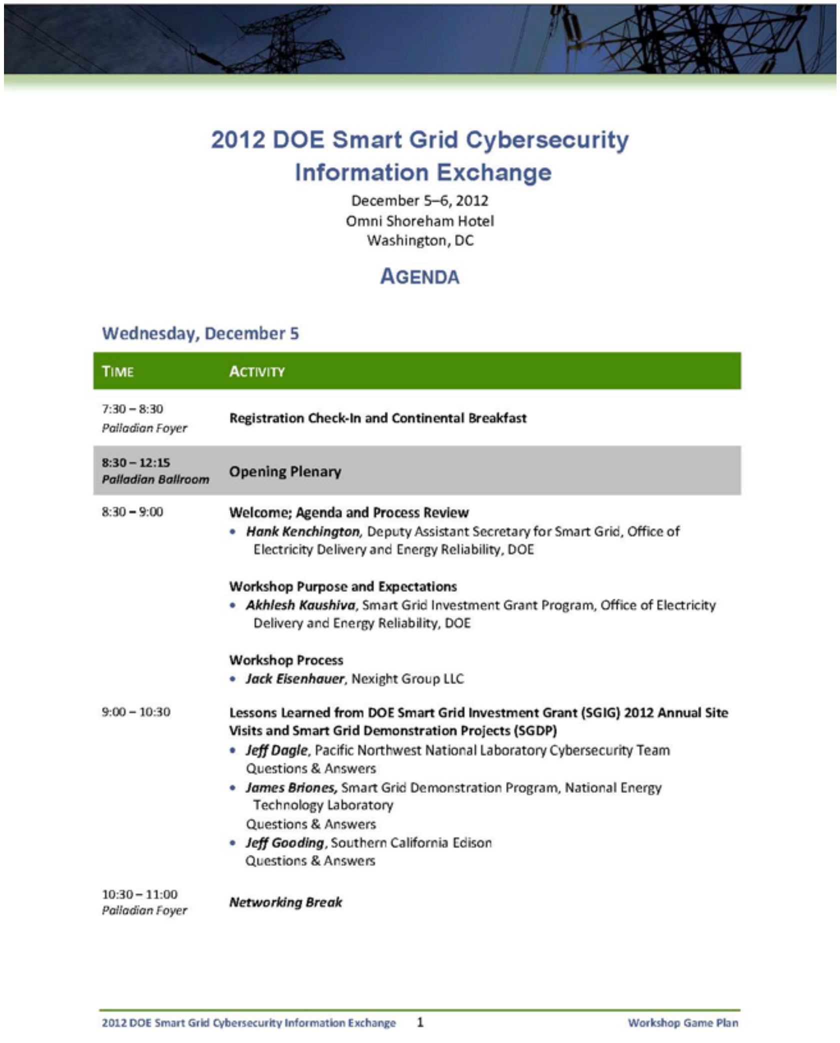
The Role of the CSP in a Post SGIG/SGDP Environment

As SGIG and SGDP projects are completed, utilities must decide how they will maintain a strong cybersecurity posture for their smart grid systems and to what extent the CSPs will contribute. The CSP, for many, was a new project management tool and how it is perceived by senior management or its ability to compete with other resource requirements is an on-going question to those who have come to recognize its value. Major points on the topic are summarized in Table 5 below.

Table 5: Challenges to CSP usage in a Post SGIG/SGDP Environment

Issue	Comments
Lack of Management “Buy-in”	• Management wonders why money needs to be spent on cybersecurity when no problem seemingly exists. • Up front management buy-in is critical so that sufficient budgets and resources are determined and not derailed when issues arise.
Issues with Company Resources	• Other resource implementation pressures put cybersecurity as a lower priority. • In some instances, utilities submitted their grant application at the inception stage of their project where they had not fully engaged in the intricacies of the cybersecurity plan and did not fully appreciate the complexity or the magnitude of the work required to become fully compliant with the cybersecurity requirements. Core elements of cybersecurity work are in competition for the same funds as other parts of the company.
Problems Implementing CSPs	• CSPs were drafted independent of other considerations resulting in conflicting expectations or timelines. o Dealing with a variety of standards and tools to test standards is sometimes a redundant process; need a unified toolset. • Initial vendor assessment is often adequate, but changes occur and there is no procurement language to capture these changes or respond to them. • Project timelines proved challenging due to lag times or delays for components caused by vendors trying to respond to rapid acceleration of smart grid procurements exceeding their capacity. • Linking the CSP for actionable information from the vendor requires the customer to do more legwork. o Due to the rapid learning curve by the vendor community maintaining alignment between requirements as stated in the CSP, their commitment to their customers and technology evolution has been challenging. o There is a lack of uniformity as it relates to cybersecurity procurement specification language between vendors and utilities especially as it relates to emerging technologies. This poses challenges for sites that are trying to ensure an unambigioious link between vendor product and CSP requirements.

APPENDIX A AGENDA



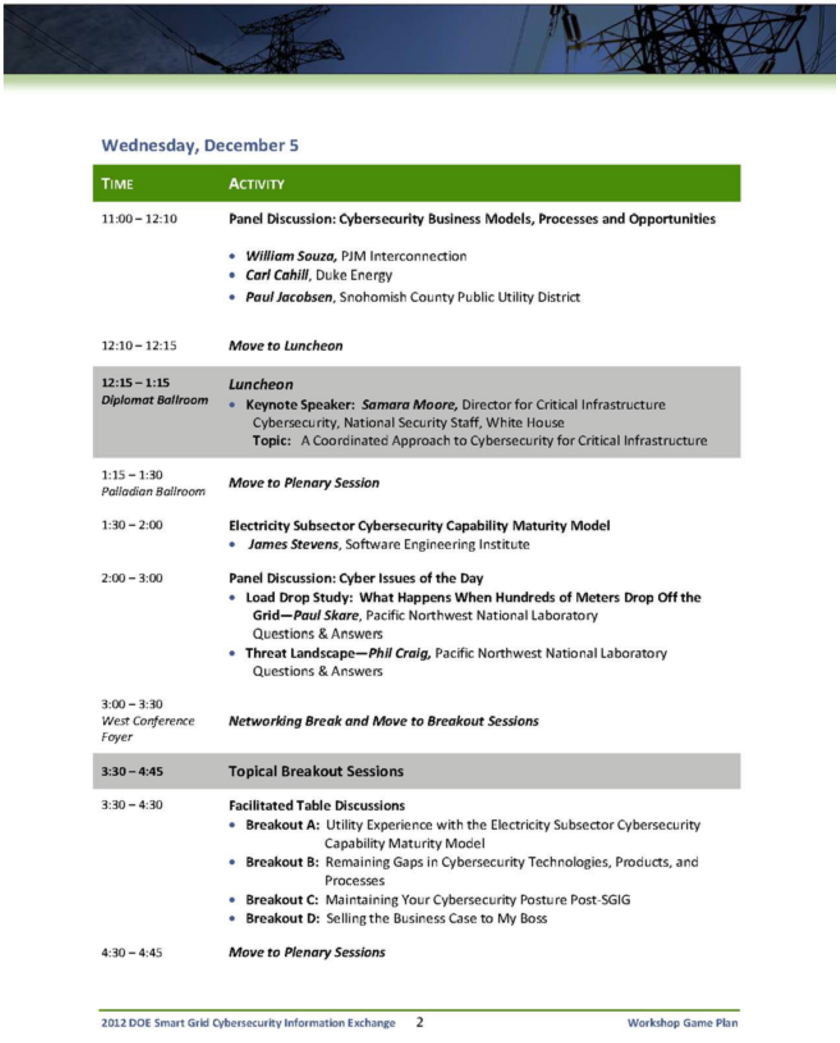
2012 DOE Smart Grid Cybersecurity Information Exchange

December 5–6, 2012
Omni Shoreham Hotel
Washington, DC

AGENDA

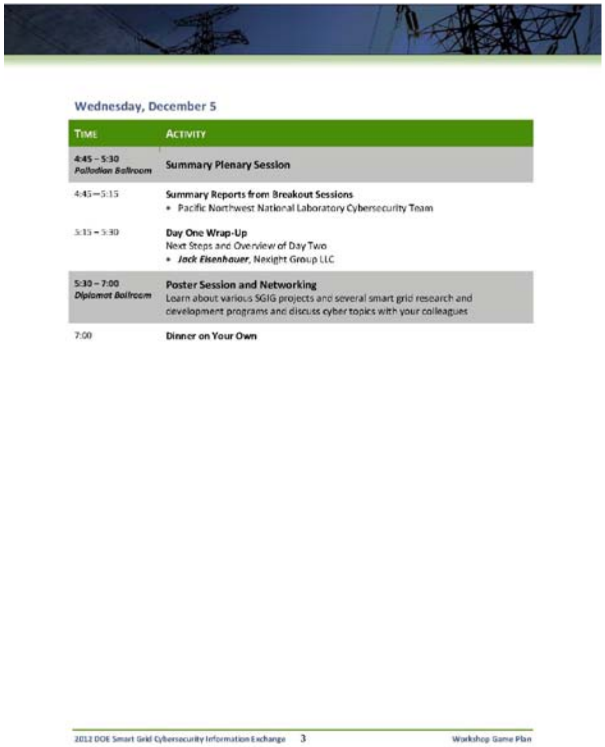
Wednesday, December 5

TIME	ACTIVITY
7:30 – 8:30 *Palladian Foyer*	**Registration Check-In and Continental Breakfast**
8:30 – 12:15 ***Palladian Ballroom***	**Opening Plenary**
8:30 – 9:00	**Welcome; Agenda and Process Review** • ***Hank Kenchington***, Deputy Assistant Secretary for Smart Grid, Office of Electricity Delivery and Energy Reliability, DOE **Workshop Purpose and Expectations** • ***Akhlesh Kaushiva***, Smart Grid Investment Grant Program, Office of Electricity Delivery and Energy Reliability, DOE **Workshop Process** • ***Jack Eisenhauer***, Nexight Group LLC
9:00 – 10:30	**Lessons Learned from DOE Smart Grid Investment Grant (SGIG) 2012 Annual Site Visits and Smart Grid Demonstration Projects (SGDP)** • ***Jeff Dagle***, Pacific Northwest National Laboratory Cybersecurity Team Questions & Answers • ***James Briones,*** Smart Grid Demonstration Program, National Energy Technology Laboratory Questions & Answers • ***Jeff Gooding***, Southern California Edison Questions & Answers
10:30 – 11:00 *Palladian Foyer*	***Networking Break***



Wednesday, December 5

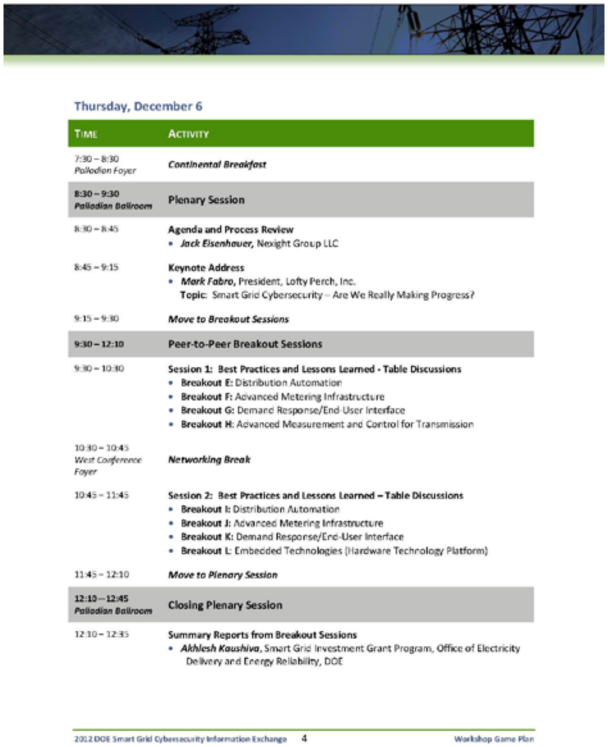
TIME	ACTIVITY
11:00 – 12:10	**Panel Discussion: Cybersecurity Business Models, Processes and Opportunities** • ***William Souza,*** PJM Interconnection • ***Carl Cahill***, Duke Energy • ***Paul Jacobsen***, Snohomish County Public Utility District
12:10 – 12:15	***Move to Luncheon***
12:15 – 1:15 ***Diplomat Ballroom***	***Luncheon*** • **Keynote Speaker:** ***Samara Moore,*** Director for Critical Infrastructure Cybersecurity, National Security Staff, White House **Topic:** A Coordinated Approach to Cybersecurity for Critical Infrastructure
1:15 – 1:30 *Palladian Ballroom*	***Move to Plenary Session***
1:30 – 2:00	**Electricity Subsector Cybersecurity Capability Maturity Model** • ***James Stevens***, Software Engineering Institute
2:00 – 3:00	**Panel Discussion: Cyber Issues of the Day** • **Load Drop Study: What Happens When Hundreds of Meters Drop Off the Grid—*Paul Skare***, Pacific Northwest National Laboratory Questions & Answers • **Threat Landscape—*Phil Craig,*** Pacific Northwest National Laboratory Questions & Answers
3:00 – 3:30 *West Conference Foyer*	***Networking Break and Move to Breakout Sessions***
3:30 – 4:45	**Topical Breakout Sessions**
3:30 – 4:30	**Facilitated Table Discussions** • **Breakout A:** Utility Experience with the Electricity Subsector Cybersecurity Capability Maturity Model • **Breakout B:** Remaining Gaps in Cybersecurity Technologies, Products, and Processes • **Breakout C:** Maintaining Your Cybersecurity Posture Post-SGIG • **Breakout D:** Selling the Business Case to My Boss
4:30 – 4:45	***Move to Plenary Sessions***



Wednesday, December 5

TIME	ACTIVITY
4:45 – 5:30 ***Palladian Ballroom***	**Summary Plenary Session**
4:45—5:15	**Summary Reports from Breakout Sessions** • Pacific Northwest National Laboratory Cybersecurity Team
5:15 – 5:30	**Day One Wrap-Up** Next Steps and Overview of Day Two • ***Jack Eisenhauer***, Nexight Group LLC
5:30 – 7:00 ***Diplomat Ballroom***	**Poster Session and Networking** Learn about various SGIG projects and several smart grid research and development programs and discuss cyber topics with your colleagues
7:00	**Dinner on Your Own**

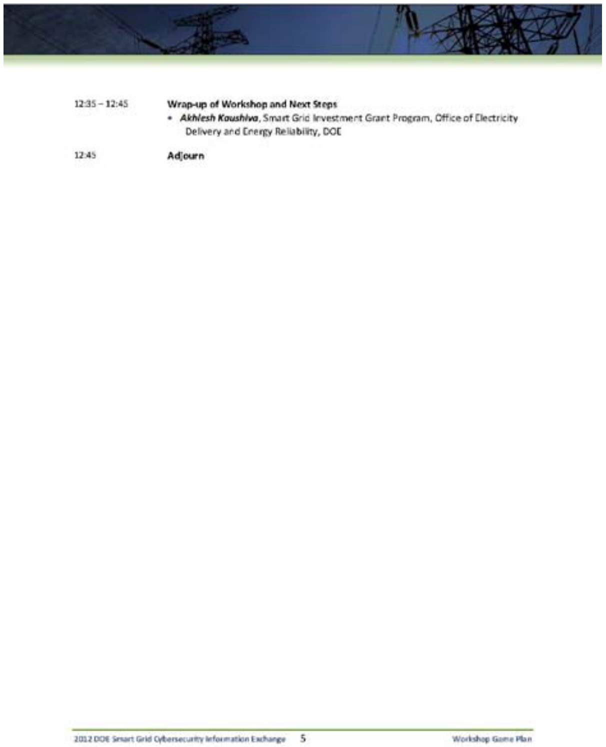
2012 DOE Smart Grid Cybersecurity Information Exchange 3 Workshop Game Plan



Thursday, December 6

TIME	ACTIVITY
7:30 – 8:30 *Palladian Foyer*	***Continental Breakfast***
8:30 – 9:30 ***Palladian Ballroom***	**Plenary Session**
8:30 – 8:45	**Agenda and Process Review** • ***Jack Eisenhauer,*** Nexight Group LLC
8:45 – 9:15	**Keynote Address** • ***Mark Fabro,*** President, Lofty Perch, Inc. **Topic:** Smart Grid Cybersecurity – Are We Really Making Progress?
9:15 – 9:30	***Move to Breakout Sessions***
9:30 – 12:10	**Peer-to-Peer Breakout Sessions**
9:30 – 10:30	**Session 1: Best Practices and Lessons Learned - Table Discussions** • **Breakout E:** Distribution Automation • **Breakout F:** Advanced Metering Infrastructure • **Breakout G:** Demand Response/End-User Interface • **Breakout H:** Advanced Measurement and Control for Transmission
10:30 – 10:45 *West Conference Foyer*	***Networking Break***
10:45 – 11:45	**Session 2: Best Practices and Lessons Learned – Table Discussions** • **Breakout I:** Distribution Automation • **Breakout J:** Advanced Metering Infrastructure • **Breakout K:** Demand Response/End-User Interface • **Breakout L:** Embedded Technologies (Hardware Technology Platform)
11:45 – 12:10	***Move to Plenary Session***
12:10 – 12:45 ***Palladian Ballroom***	**Closing Plenary Session**
12:10 – 12:35	**Summary Reports from Breakout Sessions** • ***Akhlesh Kaushiva***, Smart Grid Investment Grant Program, Office of Electricity Delivery and Energy Reliability, DOE

2012 DOE Smart Grid Cybersecurity Information Exchange 4 Workshop Game Plan



12:35 – 12:45	**Wrap-up of Workshop and Next Steps** • ***Akhlesh Kaushiva***, Smart Grid Investment Grant Program, Office of Electricity Delivery and Energy Reliability, DOE
12:45	**Adjourn**

2012 DOE Smart Grid Cybersecurity Information Exchange 5 Workshop Game Plan

Appendix B List of Participants

American Electric Power
Argonne National laboratory
Arkansas Electric Cooperative Corporation
Ashlawn Energy, LLC
Baltimore Gas and Electric
Black & Veatch
Burlington Electric Department
Burns & McDonnell Engineering Co/KCP&L
Center for the Commercialization of Electric Technologies
CenterPoint Energy
Central Lincoln PUD
City of Fulton
City of Leesburg, FL
City of Naperville
Cleco
Cobb Electric Membership Corporation
Connecticut Municipal Electric Energy Cooperative
Consolidated Edison Company of New York
Constellation Energy
Consultant
Control Center Solutions, LLC
Duke Energy
Electric Power Research Institute
EnergySec/NESCO
Entergy Services, Inc.
Florida Power & Light
Georgia System Operations Corporation
Guam Power Authority
Honeywell
Iberdrola USA Management Corp.
Iowa Association of Municipal Utilities
JEA
Lakeland Electric
Lofty Perch
Los Angeles Department of Water and Power
MEAG Power
Memphis Light Gas & Water
Navajo Tribal Utility Authority
New Hampshire Electric Cooperative
NOVEC
NOVEC / Lockheed Martin
NRG Energy, Inc.
Oncor Electric Delivery
Pacific Northwest National Laboratory
PECO
Progress Energy
Rappahannock Electric Cooperative
Sacramento Municipal Utility District
San Diego Gas and Electric
Snohomish County PUD
South Kentucky RECC
South Mississippi Electric Power Assn.
Southern California Edison
Southwest Research Institute
Southwest Transmission Cooperative, Inc.
Stroz Friedberg
Sulphur Springs Valley Electric Cooperative
Talquin Electric Cooperative
TCIPG/University of Illinois
The Flynt Group, Inc.
True Digital Security
U.S. Department of Energy
U.S. Department of Energy-NETL
University of Illinois at Urbana-Champaign
Woodruff Electric Cooperative Corp.