



CyberCap & Smart Grid Cyber Security Workshop

Date: 8/19-20/2010
 Time: 7:30am-4:30pm 8/19 and 8:00am-2:00pm 8/20
 Conference Room: Austin
 Place: Sheraton Dallas Hotel

Workshop Organizer Department Of Energy – Office of Electricity Delivery & Energy Reliability Infrastructure Security & Energy Restoration (ISER)

Type of meeting: CyberCap & Smart Grid Cybersecurity Workshop

Purpose: The CyberCap & Smart Grid Cyber Security Workshop offers an opportunity to talk with DOE National Lab experts on cyber security and control systems security. Whether you need help in analyzing threats, recognizing and responding to an attack, conducting forensics, or partnering with a lab to conduct research in cyber or smart grid cyber security, the CyberCap & Smart Grid Cyber Security Workshop will offer you direction and insights. In addition, participants will learn about an interface that will allow for quick searches on specific cyber security capabilities at the labs. You will also have an opportunity to learn about the latest on cyber security standards and best practices, and to provide feedback on DOE’s Smart Grid Cybersecurity strategy.

Resource person: Logistics: Cindy Taylor 304-285-4750
 Technical Coordinator: James Briones 304-276-5293

Workshop Agenda

Day 1: August 19, 2010

CyberCap: Accessing the DOE National Laboratory Capabilities

7:30	Sign in and Assemble in Conference Room (Continental Breakfast)	All
8:30	Introductions/Welcome/Workshop Purpose	Rhonda Dunfee and Diane Hooie
8:45	CyberCap SharePoint Site Presentation	James Briones
9:00	Control Systems Cybersecurity Advanced Training	Idaho National Laboratory
9:30	Cyber Federated Model	Argonne National Laboratory
10:00	Break	All
10:30	CyberSim – Consequence-based Scalable Simulation and Visualization Suite	Los Alamos National Laboratory
11:00	Behavior-based Anomaly Detection	Oak Ridge National Laboratory
11:30	Secure SCADA Communications Protocol	Pacific Northwest National

		Laboratory
12:00	Working Lunch Collaboration Success Story	Sharla Artz, Director Government Affairs, SEL
1:30	CICM-Critical Infrastructure Consequence Modeler	Sandia National Laboratory
2:00	SCADA/EMS Cybersecurity Assessment	Idaho National Laboratory
2:30	Break	
3:00	GridLab-D	Pacific Northwest National Laboratory
3:30	SEEPS: Simulation Engine for Electric Power Systems	Oak Ridge National Laboratory
4:00	IDART-Information Design Assurance	Sandia National Laboratory
4:30	Closing Remarks/How to Access CyberCap SharePoint Site	Rhonda Dunfee
5:00	Adjourn	
Day 2: August 20, 2010 <i>Addressing Smart Grid Cyber Security</i>		
7:30	Registration/Assemble in Conference Room (Continental Breakfast)	All
8:30	DOE Panel: Experience with Smart Grid <i>DOE is responsible for investing \$4.5 billion in a nationwide plan to modernize the electric power grid. DOE has developed a body of cybersecurity work that can be applied to today's modernization efforts.</i> Security Attributes of Smart Grid (Recommendations to Government/Industry) Cybersecurity Plan Best Practices Cybersecurity for Smart Grid Applications Working with DoD on Energy Assurance	Jeff Dagle, Moderator PNL PNL TCIPG – Bill Saunders SNL
9:15	Industry Panel: Lessons Learned from Implementing Smart Grid <i>The ARRA Smart Grid Investment Grant Awardees have developed cybersecurity plans for their programs and have begun implementation of their projects.</i>	Don MacDonald, Moderator
10:00	Break	All
10:15	States PUC/PSC Panel: Experience with Smart Grid Implementation <i>Many states are making progress in engaging their</i>	Tom Pearce, Moderator

	<p><i>utilities on Smart Grid and advancing cybersecurity issues. They recognize the potential benefits, such as fewer new power plants and cleaner air, while ensuring utilities consider grid security and cybersecurity</i></p> <p>Overall efforts Texas Lessons Learned</p>	<p>NARUC Texas PUC</p>
11:00	<p>Standards Organizations Panel: Bringing together Smart Grid Security Standards and Guidelines</p> <p><i>There are many efforts underway to develop standards and guidelines for Smart Grid security. The following organizations are working to develop needed standards and determine how to bring them together.</i></p> <p>Smart Grid Interoperability Panel-Cybersecurity Working Group (CSWG) SG Security Working Group Advanced Security Acceleration Project for the Smart Grid (ASAP-SG) NERC CIP Standards</p>	<p>Darren Highfill, Moderator</p> <p>NIST EnerNex SEI CIP Standards Drafting Team</p>
12:00	<p>Working Lunch Next Steps for Smart Grid Cybersecurity</p>	<p>Michael Assante President & CEO, National Board of Information Security Examiners (NBISE)</p>
1:15	<p>Discussion on DOE's Smart Grid Cybersecurity Strategy</p> <p><i>Many different organizations and government agencies conduct Smart Grid activities. DOE is a major stakeholder in the expansion of the Smart Grid and is developing a Smart Grid Cybersecurity Strategy. This session presents the participants an opportunity to provide input and feedback to the strategy.</i></p>	<p>Bill Huntman</p>
2:00	<p>Adjourn</p>	