AGENDA

Cybersecurity for Energy Delivery Systems
2010 Peer Review

July 20-22, 2010
Westin Alexandria ● Alexandria, VA

Tuesday, July 20 – Day 1		
Time	Activity	Host/Presenter
7:30 – 8:30 am	Registration and Continental Breakfast	
8:30 – 8:45 am	Welcome from Program Manager	Carol Hawk
8:45 – 9:00 am	Introductions and Instructions	Katie Jereza
Best Practices/Standards Development		
9:00 – 9:30 am	**Advanced Security Acceleration Project for the Smart Grid (ASAP-SG)**	Oak Ridge National Laboratory
9:30 – 10:00 am	**Lemnos Interoperable Security**	EnerNex Corporation
10:00 – 10:30 am	**Trustworthy Wireless for Critical Infrastructure Sites**	Oak Ridge National Laboratory
10:30 – 11:00 am	BREAK	
Best Practice Design/Configuration		
11:00 – 11:30 am	**Field Device Management**	Pacific Northwest National Laboratory
11:30 – 12:00 pm	**Implications of Design Basis Threat on Critical Infrastructure Protection and Homeland Security**	Pacific Northwest National Laboratory
12:00 – 12:30 pm	**Cyber Security Audit and Attack Detection Toolkit**	Digital Bond
12:30 – 2:30 pm	LUNCH	
Visualization and Modeling		
2:30 – 3:00 pm	**Real-Time Security State Visualization Tool**	Pacific Northwest National Laboratory
3:00 – 3:30 pm	**Hard Problems Analysis (VCSE Validation)**	Sandia National Laboratories
3:30 – 4:00 pm	BREAK	
4:00 – 4:30 pm	**Threat Characterization**	Sandia National Laboratories
4:30 – 5:00 pm	**Reliability Impacts for Cyber Attack (RICA)**	Sandia National Laboratories
5:00 – 7:00 pm	POSTER SESSION with light appetizers and cash bar	

Wednesday, July 21 – Day 2		
Time	Activity	Host/Presenter
7:30 – 8:30 am	Continental Breakfast	
Software Engineering Institute		
8:30 – 9:00 am	**CERT OCTAVE BES – Guidance in Identifying and Managing Electricity Sector Risk**	Carnegie Mellon University Software Engineering Institute
9:00 – 9:30 am	**SCADA Source Code Analysis and Conformance Testing – Source Code Analysis Laboratory (SCALe)**	Carnegie Mellon University Software Engineering Institute
9:30 – 10:00 am	**Adapting the CERT Resilience Management Model to the Electricity Sector**	Carnegie Mellon University Software Engineering Institute
10:00 – 10:30 am	BREAK	
Vulnerability and Intrusion Detection		
10:30 – 11:00 am	**Control Systems Vulnerability Assessments**	Idaho National Laboratory/Argonne National Laboratory
11:00 – 11:30 am	**Integrated Security System**	Siemens Corporate Research
11:30 – 12:00 pm	**Protecting Process Control Systems against Lifecycle Attacks Using Trust Anchors**	Sandia National Laboratories
12:00 – 2:00 pm	LUNCH	
Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)		
2:00 – 2:30 pm	**TCIPG Overview**	TCIPG
2:30 – 3:00 pm	**COnverged NEtworks for SCADA (CONES)**	TCIPG
3:00 – 3:30 pm	BREAK	
3:30 – 4:00 pm	**Smart Grid Distributed Voltage and Reactive Power Control**	TCIPG
4:00 – 4:30 pm	**GridStat**	TCIPG
4:30 – 5:00 pm	**Network Access Policy Tool (NetAPT)**	TCIPG

Thursday, July 22 – Day 3		
Time	Activity	Host/Presenter
7:30 – 8:30 am	Continental Breakfast	
	Secure Communications	
8:30 – 9:00 am	**Cryptographic Trust Management**	Pacific Northwest National Laboratory
9:00 – 9:30 am	**Right-Sized SCADA Communication**	Los Alamos National Laboratory
9:30 – 10:00 am	**Sophia**	Idaho National Laboratory
10:00 – 10:30 am	BREAK	
10:30 – 11:00 am	**Hallmark Cryptographic Serial Communication**	Schweitzer Engineering Laboratories
11:00 – 11:30 am	**SSCP Commercialization**	Pacific Northwest National Laboratory
11:30 – 12:00 pm	**Protocol Analyzer**	Pacific Northwest National Laboratory
12:00 – 12:30 pm	**Secure Communications Architecture for the Energy Sector**	Pacific Northwest National Laboratory
12:30 pm	PEER REVIEW ADJOURNS	