

<b>DAY 1 - Tuesday, April 6, 2010</b>			
7:00 - 8:00	<b>Registration</b>		
8:00 - 8:30	<b>Welcome and Keynote</b> Sean McGurk and Tim Roxey ICSJWG Co-Chairs		
8:30 - 9:00	<b>National Cybersecurity and Communications Integration Center</b> Preston Wernitz, DHS		
9:00 - 9:15	Break		
9:15 - 9:45	<b>Vendor Subgroup Meeting - Open</b> Rick Lichtenfels, GCC and Eric Cosman, SCC		
9:45-10:15	<b>Workforce Development Subgroup Meeting - Open</b> Ben Wible, GCC and Marcus Sachs, SCC		
10:15 - 10:30	Break		
10:30 - 11:00	<b>Information Sharing Subgroup Meeting - Open</b> George Bamford, GCC and Nathan Faith, SCC		
11:00 - 11:30	<b>International Subgroup Meeting - Open</b> Sean McGurk, GCC and Michael Assante, SCC		
11:30 - 12:45	Lunch		
12:45 - 1:15	<b>Research and Development Subgroup Meeting - Open</b> Douglas Maughan, GCC and David Norton, SCC		
1:15 - 1:45	<b>ICS Roadmap Development Subgroup Meeting - Open</b> Perry Pederson, GCC and Tim Roxey, SCC		
1:45 - 2:00	Break		
Presentations	<b>Policy and Standards</b>	<b>Technology</b>	<b>Case Studies</b>
2:00 to 2:45	<b>Matthew Luallen,</b> Encari <i>Lessons Learned Performing Cyber Asset Discovery at Generating Facilities</i>	<b>Phillip Hallam-Baker,</b> Default Deny Security Inc. <i>Defeating Malicious Code</i>	<b>Bradford Willke,</b> Dept. of Homeland Security <i>Cyber Resiliency Review - Evaluation Methodology</i>
2:45 - 3:00	Break		
3:00 - 4:30	<b>SCC Break-out Meeting</b> Tim Roxey	<b>GCC Break-out Meeting</b> Sean McGurk	<b>Zach Tudor,</b> SRI International <b>Mark Fabro,</b> Lofty Perch <i>What Went Wrong? A Study of Actual Industrial Cyber Security Incidents</i>

<b>DAY 2 - Wednesday, April 7, 2010</b>			
7:00 - 8:00	<b>Registration</b>		
Presentations	<b>Policy and Standards</b>	<b>Technology</b>	<b>Case Studies</b>
8:00 - 8:45	<b>Peter Kwaspen,</b> Shell <b>Tyler Williams,</b> Wurdtech <i>Functional Cyber Security Best Practices Certification Program: An Update for Industrial Stakeholders</i>	<b>Sean McBride,</b> Critical Intelligence <b>Rick Howard,</b> iDefense Intelligence <i>Intelligence 2010 for Critical Infrastructure</i>	<b>Joe Weiss,</b> Applied Control Solutions, LLC <i>The Need to Connect the Dots on ICS Cyber Incidents</i>
8:45 - 9:00	Break		

DAY 2 - Wednesday, April 7, 2010 - continued			
Presentations	Policy and Standards	Technology	Case Studies
9:00 - 9:45	<b>Andre Ristaino</b> , ISCI <b>Thomas Culling</b> , Chevron <b>Paul Forney</b> , Invensys <b>John Cusimano</b> , Exida <i>The Role of Product Certification in an Overall Cyber Security Strategy</i>	<b>Ernest Rakaczky</b> , Invensys <b>Charles Ross</b> , McAfee <i>Applying Current Security Technology for Endpoint Protection, Host Intrusion Prevention for DCS</i>	<b>Brian Smith</b> , EnerNex Corporation <i>The Lemons Interoperable Security Project</i>
9:45 - 10:00	<b>Break</b>		
10:00 - 10:45	<b>Eric Cosman</b> , ISA <i>Setting Up a Patch Management Program for ICS</i>	<b>Andrew Ginter</b> , Industrial Defender <i>Experience with Network Anomaly Detection on Industrial Networks</i>	<b>Emily Frye</b> , SRA International <b>Alan Hendricks</b> , SRA International <i>Harnessing the Power of Visualization for Control System Cybersecurity</i>
10:45 - 11:00	<b>Break</b>		
11:00 - 11:45	<b>Joy Renfro</b> , USACE <b>Bart Rylander</b> , USACE US Army Corps of Engineers <i>Securing a Legacy SCADA System</i>	<b>Steven Venema</b> , Boeing <i>SCADAnet: A Standards-Based Practical Solution for Securing ICS</i>	<b>Clint Kreitner</b> , CIS <b>Sharon Xia</b> , AREVA <b>Mike Assante</b> , NERC <b>Dale Peterson</b> , Digital Bond, Inc. <b>Stephen Hilt</b> , TVA <i>Control Systems Security: A Case Study in Collaboration</i>
11:45 - 1:15	<b>Lunch</b>		
1:15 - 2:00	<b>Jerald Dawkins</b> , True Digital Security <i>Beyond Regulatory Compliance Toward a Comprehensive Security Program</i>	<b>James Davidson</b> , Idaho National Laboratory <i>Sophia: Tool development for ICS Security</i>	<b>Eric Byres</b> , Byres Security Inc. <i>Fingers Burned and Lessons Learned: Securing Modbus TCP and OCP with Deep Packet Inspection Technologies</i>
2:00 - 2:15	<b>Break</b>		
2:15 - 3:00	<b>Joel Langill</b> , ENGlobal Automation <i>Incorporating Cybersecurity into Your Automation Project's Execution Methodology</i>	<b>Pan Kamal</b> , AlertEnterprise, Inc <i>The Silent Risk We're Living with Using Convergent Risk Analysis to Uncover Insider Threats</i>	<b>Bernie Pella</b> , Savannah River Nuclear Solutions <i>Scanning a Clone in the Cloud; Safe DCS Vulnerability Scanning</i>
3:00 - 3:15	<b>Break</b>		
3:15 - 4:00	<b>Justin Harvey</b> , Encari <i>Strategic Identity Management in Industrial Control Systems</i>	<b>Robert Sill</b> , RealTime Interactive Systems <i>Securing Serial Communications in Electric Industry Substations</i>	<b>John Cusimano</b> , Exida <i>Evaluating the Safety and Security of Automation Products, Systems, and Suppliers</i>
4:00 - 4:15	<b>Break</b>		
4:15 - 5:00	<b>Walter Sikora</b> , Industrial Defender <i>Safety Considerations for SCADA/DCS Cybersecurity</i>	<b>Hirmanshu Khurana</b> , University of Illinois <i>Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols</i>	<b>Ragnar Schierholz</b> , ABB Corporate Research <i>Evaluation of ISA 99 in a Real-World Power Plant Security Assessment</i>
5:00 - 5:15	<b>Closing Remarks and Wrap-up</b> Sean McGurk - Tim Roxey		
5:15	<b>Adjourn</b>		

<b>DAY 3 - Thursday, April 8, 2010</b> <b>Training: Introduction to Cybersecurity for Control Systems</b>	
8:00 - 8:15	<b>Welcome and Introductions</b>
8:15 - 10:00	<b>Session 1 - Cyber Security Landscape: Understanding the Risks</b>
10:00 - 10:15	<b>B r e a k</b>
10:15 to 12:00	<b>Session 2 - Industrial Control Systems and Applications</b>
12:00 to 1:15	<b>L u n c h</b>
1:15 - 3:00	<b>Session 3 - Current State of Cybersecurty in Industry</b>
3:00 - 3:15	<b>B r e a k</b>
3:15 - 5:00	<b>Session 4 - Practical Application of Cybersecurity</b>