



### **ICSJWG Fall Conference, Idaho Falls, ID**

The Industrial Control Systems Joint Working Group 2009 Fall Conference will be held at the Hilton Garden Inn on November 3–5, 2009, in Idaho Falls, Idaho. This event will provide control systems stakeholders from industry, government, academia, international, vendor, and research and development communities with an opportunity to network and engage in discussions related to securing control systems. Registration and additional information are at <https://secure.inl.gov/icsjwg-conference/>

**Optional Tour on November 6, 2009.** For interested individuals, the Idaho National Laboratory will provide a 4-hour tour of the Experimental Breeder Reactor I, a decommissioned research reactor and U.S. National Historic Landmark.

### **ICSJWG Subgroups**

At the ICSJWG Inaugural Symposium, critical issues were identified as key to developing a program for secure control systems. ICSJWG members voted to establish the following six subgroups, all of which have been chartered under the ICSJWG and NIPP framework. Many of the subgroups are soliciting volunteers to join in their efforts.

#### **Information Sharing Subgroup**

**Co-Chairs:** George Bamford ([george.bamford@dhs.gov](mailto:george.bamford@dhs.gov)) and Nathan Faith ([nlfaith@aep.com](mailto:nlfaith@aep.com)). The Information Sharing Subgroup was formed to address challenges and priorities related to sharing ICS cybersecurity information and integrating control systems asset owners, operators, vendors, and other stakeholders into a nationwide operational cyber risk management capability. Key milestones are:

- Document current information sharing mechanisms and prepare recommendations for addressing gaps
- Document existing vulnerability reporting procedures and deficiencies
- Prepare a recommendations guide for addressing the identified gaps, improving vulnerability disclosure, and implementing mitigation strategies
- Develop a clear set of reporting and incident handling guidelines.

### **About the ICSJWG**

*The ICSJWG is a collaborative and coordinating body operating under the Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure and key resources (CIKR) sectors between federal agencies and departments as well as private asset owner/operators of industrial control systems. The goal of the ICSJWG is to continue and enhance the facilitation and collaboration of the industrial control systems stakeholder community in securing CIKR by accelerating the design, development, and deployment of secure industrial control systems.*

*For more information, visit [http://www.us-cert.gov/control\\_systems/icsjwg/](http://www.us-cert.gov/control_systems/icsjwg/)*

## **International Subgroup**

**Co-Chairs:** Seán McGurk ([cssp@dhs.gov](mailto:cssp@dhs.gov)) and Michael Assante ([michael.assante@nerc.net](mailto:michael.assante@nerc.net)).

The International Subgroup was formed to address the growing need for international coordination and collaboration to effectively manage cyber risk in control systems environments both domestically and abroad. Key milestones are:

- Prepare a comprehensive “players” manual of international CERTs and their organization’s contact and focus information
- Prepare a communications plan for international collaboration.
- Document available collaboration tools, including a gap analysis to identify needed enhancements
- Document and identify international document handling/classification standards and perform a feasibility study for developing a common lexicon.

## **Research and Development Subgroup**

**Co-Chairs:** Dr. Douglas Maughan ([Douglas.Maughan@dhs.gov](mailto:Douglas.Maughan@dhs.gov)) and David L Norton ([DNORTO1@entergy.com](mailto:DNORTO1@entergy.com)).

The Research and Development Subgroup was formed to facilitate communication between industrial control systems stakeholders and the research and development community to ensure effective focus for research and development initiatives and associated funding. Key milestones are:

- Document current and planned projects with associated details, timelines, and stakeholder involved
- Document results of an ICS research and development needs assessment
- Prepare a requirements document for sharing sensitive information including an ultimate recommendation as to whether or not a new tool is needed.

## **Roadmap to Secure Industrial Control Systems**

**Co-Chairs:** Seán McGurk ([cssp@dhs.gov](mailto:cssp@dhs.gov)) and Tim Roxey ([Tim.Roxey@nerc.net](mailto:Tim.Roxey@nerc.net)).

The Roadmap to Secure ICS Subgroup was formed to create a strategic plan to address the high-level management of cyber risk within control systems environments. Key milestones are:

- Document common threads for ICS challenges, priorities, and objectives across all infrastructure sectors for input to the ICS Roadmap
- Prepare a gap analysis to identify areas that need to be addressed
- Prepare a draft roadmap.

## **Vendor Subgroup**

**Co-Chairs:** Seán McGurk ([cssp@dhs.gov](mailto:cssp@dhs.gov)) and Eric Cosman ([ECCosman@dow.com](mailto:ECCosman@dow.com)).

The Vendor Subgroup was formed to address challenges and discuss issues related to managing risk associated with control systems products and services. Key milestones are:

- Document stakeholder groups, challenges, and equities
- Prepare recommendations that address all groups and areas of concerns.

## **Workforce Development Subgroup**

**Co-Chairs:** Ben Wible ([wibleb@ndu.edu](mailto:wibleb@ndu.edu)) and Marcus Sachs ([marcus.sachs@verizon.com](mailto:marcus.sachs@verizon.com)).

The Workforce Development Subgroup was formed to address challenges and priorities related to personnel awareness of cybersecurity issues within control systems environments and development of skills for more effective cyber risk management. Key milestones are:

- Prepare a gap analysis of control systems security workforce capabilities and development opportunities

- Prepare a feasibility study for a control systems security certification program
- Develop knowledge domain areas for a certification program
- Develop a control systems security workforce outreach plan.

To learn more or get involved with any of these subgroups, e-mail one of the group co-chairs or e-mail [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov).

### **Contact Information**

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an e-mail to [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov).

The CSSP and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at <https://forms.us-cert.gov/report/>.

Other important contact information:

Web Site Address: [http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)

ICS-CERT Email: [ics-cert@dhs.gov](mailto:ics-cert@dhs.gov)

Phone: 1-877-776-7585

CSSP Email: [cssp@dhs.gov](mailto:cssp@dhs.gov)