



### **ICSJWG 2009 Fall Conference**

The Industrial Control Systems Joint Working Group (ICSJWG) 2009 Fall Conference was held on November 3–5 in Idaho Falls, Idaho. Control systems stakeholders from industry, government, academia, international, vendor, and research and development communities engaged in discussions related to securing control systems and attended presentations related to control systems products, data analysis approaches, case studies, and policy issues.

ICSJWG subgroup co-chairs presented to all conference participants on the progress of their subgroups, discussed key issues, and fielded questions. Volunteers are still needed to join and support the efforts of the subgroups. Below is a brief summary of the discussions that took place.

#### **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 addresses challenges and priorities related to information sharing and the integration of control systems asset owners, operators, vendors and other stakeholders into a nationwide operational cyber risk management capability.

The Information Sharing subgroup discussion focused on the need to establish trusted relationships in order to facilitate information sharing. Several proposals were put forward to address this goal:

- Create a control systems security information exchange similar to that of the European SCADA and Control Systems Information Exchange, established by the UK for the European community
- Establish a mechanism to clear on-site technical cyber security personnel to facilitate information sharing in real time
- Focus on preventative instead of reactionary information sharing
- Conduct an analysis of incidents that could have been prevented if more information sharing had occurred

More information about the subgroup including its charter, goals, and objectives can be found at [http://www.us-cert.gov/control\\_systems/pdf/Information\\_Sharing\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/Information_Sharing_Subgroup_Charter.pdf).

#### **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 addresses the growing need for international coordination and collaboration to effectively manage cyber risk in control systems environments both domestically and abroad. The subgroup discussion focused on the following proposals:

- The subgroup will incorporate a ‘lessons learned’ process into the international coordination and collaboration efforts
- The subgroup will strive to incorporate key representatives from around the globe
- The subgroup will assess the usefulness of the stoplight protocol in international collaboration

More information about the subgroup including its charter, goals, and objectives can be found at: [http://www.us-cert.gov/control\\_systems/pdf/International\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/International_Subgroup_Charter.pdf).

## **Research and Development Subgroup**

**Co-Chairs:** Dr. Douglas Maughan ([Douglas.Maughan@dhs.gov](mailto:Douglas.Maughan@dhs.gov)) and Dave “Nort” Norton ([DNORTO1@entergy.com](mailto:DNORTO1@entergy.com)).

The Research and Development Subgroup facilitates communication between industrial control systems stakeholders and the research and development community by effectively focusing research and development initiatives and associated funding.

The co-chairs described early thinking about the scope, orientation, and goals for the subgroup. A major objective is identification of control systems security needs that can be addressed through research and development, based largely on input from critical infrastructure control systems owners and operators. Another area of need, which the subgroup may be able to assist, is defining testing and evaluation requirements for products felt to be ready for transition from the research process to operational implementation. Through the DHS Office of Science and Technology, the subgroup will facilitate communication with the greater control systems research and development community, including activities under the aegis of the National Science Foundation and the DOE “ieRoadmap to Secure Control Systems.” The subgroup will emphasize aligning efforts in order to both leverage related research activity and avoid redundancy. The session concluded with an invitation to attendees to contact one of the co-chairs if interested in active participation in the subgroup.

The co-chairs challenged the audience to identify control systems research and development requirements that require attention. Some of the areas identified were:

- Improvements to the Internet Protocol stack
- Identity management
- Large scale digital certificate management for unmanned intelligent networked devices
- The need to define minimum-set requirements for secure interoperability between legacy and emergent control system equipment
- Forensics research focused on criminal activity involving control systems
- Needs analysis for control system interdependencies across industrial infrastructure environments

- Incorporation of deceptive technologies into control systems
- Robust specifications for secure wireless capabilities integrated into vendor product implementations

The Subgroup plans to conduct periodic virtual meetings with quarterly updates from the co-chairs and semi-annual meetings during the ICSJWG conferences. More information about the subgroup including its charter, goals, and objectives can be found at: [http://www.us-cert.gov/control\\_systems/pdf/R&D\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/R&D_Subgroup_Charter.pdf).

### **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 will create a strategic plan to address the high-level management of cyber risk within control systems environments.

The co-chairs discussed the need to evaluate existing roadmaps for common issues or challenges shared by the various sectors. A template and preparation guide for an ICS roadmap has been prepared and is available to subgroup participants. The ICS roadmap will seek to:

- Measure and assess security posture
- Integrate common issues and challenges
- Develop and integrate protective measures
- Detect intrusions and implement response strategies
- Sustain security improvements
- Facilitate partnership and outreach
- Enhance security and control by design
- Identify cross-sector specific issues and challenges

The roadmap will draw from existing roadmaps such as the Energy, Water, and Chemical, as well as the Nuclear and Dams sector roadmap efforts, which are currently underway. The planned roadmap will capture the detail necessary to address cross-section ICS security and will refer back to Sector Specific Plans for consistency. The co-chairs will also leverage the efforts of international partners and other subgroups where appropriate. As the work of the subgroup moves forward, the ICSJWG Program Office will facilitate regular meetings. More information about the subgroup including its charter, goals, and objectives can be found at: [http://www.us-cert.gov/control\\_systems/pdf/Roadmap\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/Roadmap_Subgroup_Charter.pdf).

### **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 addresses challenges and issues related to managing risk associated with control systems products and services.

The co-chairs have conducted three conference calls over the past several months and a strong nucleus of participating members has been established. The subgroup will continue to address challenges and issues related to secure product design, vulnerability management, and risks that have cross-sector impacts associated with control systems products and services.

The subgroup will conduct monthly conference calls and meet in person at ICSJWG general meetings. More information about the subgroup including its charter, goals, and objectives can be found at: [http://www.us-cert.gov/control\\_systems/pdf/Vendor\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/Vendor_Subgroup_Charter.pdf).

### **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 addresses challenges and priorities related to personnel awareness of cybersecurity issues within control systems environments and development of skills for more effective cyber risk management.

The co-chairs presented findings from recent efforts to identify curricula and develop recommendations to enhance or create new curriculum. The co-chairs also discussed the work currently underway to accomplish the goals of the subgroup including a web portal for subgroup communications. The goals of the subgroup are focused on workforce development at the entry level, as well as improving awareness and practices among well-established control system professionals. Additionally, the subgroup is evaluating the need for licensing and/or certification programs to address life safety issues associated with cybersecurity.

The co-chairs are seeking individuals who may be interested in providing their unique insights and experiential knowledge regarding curriculum development and certification of the workforce.

More information about the subgroup including its charter, goals, and objectives can be found at: [http://www.us-cert.gov/control\\_systems/pdf/Workforce\\_Development\\_Subgroup\\_Charter.pdf](http://www.us-cert.gov/control_systems/pdf/Workforce_Development_Subgroup_Charter.pdf).

### ***Participation is Key!***

Your participation and input is **critical** to the success of these subgroups and to the overall mission of ICSJWG to coordinate cybersecurity efforts to secure ICS across the nation's critical infrastructure. Please email the co-chairs or [icsjwg@dhs.gov](mailto:icsjwg@dhs.gov) to get involved with one or more of the subgroups.

### ***DHS Assistant Secretary Schaffer Dedicates New ICS-CERT Facility***

On November 3, 2009, DHS officially launched the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) facility with a dedication ceremony led by DHS Assistant Secretary for Cybersecurity and Communications Greg Schaffer in Idaho Falls, Idaho.

The [ICS-CERT](#) is the Nation's first dedicated response center aimed at reducing the frequency and effect of cyber attacks on industrial control systems. ICS-CERT monitors, collects, and analyzes cyber incidents reported by industrial control systems stakeholders across all sectors of the nation's critical infrastructure.

The ICS-CERT was created earlier this year to coordinate global efforts and respond to cyber vulnerabilities and threats affecting the industrial control systems that operate critical infrastructure and key resources.

The ICS-CERT is a key component of [The Strategy for Securing Control Systems](#) and provides capabilities to:

- Respond to and analyze control system related incidents
- Conduct control system related vulnerability and malware analysis
- Provide onsite support for control system related forensic investigations
- Provide situational awareness in the form of actionable intelligence
- Coordinate the responsible disclosure of control systems vulnerability information in partnership with the vendor community.

Through its participation in the Industrial Control Systems Joint Working Group, the ICS-CERT forges trusted relationships with private sector owner operators and vendors as well as Federal owners and operators to reduce risk to industrial control systems.

### ***Save the Date- ICSJWG Spring Conference***

The ICSJWG Spring Conference will be held on April 6-8, 2010 in San Antonio, Texas at the JW Marriott San Antonio Hill Country Hotel and Conference Center. The conference will include presentations by industry leaders in control systems cybersecurity, updates from the ICSJWG Subgroups, and the *Introduction to Industrial Control Systems Cybersecurity* training course.

Conference details, a call for papers, and registration information will be available soon at [http://www.us-cert.gov/control\\_systems/icsjwg/index.html](http://www.us-cert.gov/control_systems/icsjwg/index.html).

### ***Advanced Training Events Scheduled for 2010***

The following advanced training events have been scheduled for 2010:

- March 1-5, 2010 - Asset Owners and Operators
- April 12-16, 2010 – International Partners

The training is held at the Control Systems Analysis Center located in Idaho Falls, Idaho and will provide intensive hands-on training on protecting and securing industrial control systems from cyber attacks, including a Red Team/Blue Team exercise that will be conducted within an actual control systems environment.

There is no cost to attend the training; however, travel expenses and accommodations are the responsibility of each participant. More information, including registration will be posted to [http://www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/) in the near future.

### ***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 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)