



ICSJWG Past Events

Inaugural Symposium, Denver, CO

The Industrial Control Systems Joint Working Group (ICSJWG) held its inaugural symposium in March in Denver, CO. The meeting was a great success with over 100 invitees participating from both government and the private sector and representing several critical infrastructure key resource (CIKR) sectors. As a result, the ICSJWG has commissioned the formation of six subgroups; Information Sharing, International, Research and Development, ICS Roadmaps, Vendor, and the Workforce Development.

May Federal Partners and ICSJWG Meeting

A working meeting was also conducted on May 19 at the Control Systems Security Program (CSSP) offices in Arlington, VA to discuss the scope, objectives, and milestones of each subgroup's draft charter. Approximately 30 ICSJWG members attended and the basic objectives of each subgroup were approved and will be finalized when the charters are completed and issued later this month.

ICSJWG Subgroups

As mentioned above, the ICSJWG Inaugural Symposium resulted in the formation of the following subgroups.

Information Sharing Subgroup

The Information Sharing Subgroup will develop recommendations to facilitate greater information sharing of vulnerabilities and threats to control systems among industry, vendors, and public sector. The Subgroup will work to improve the vulnerability management processes and create incident reporting and handling guidance.

International Subgroup

The International Subgroup will focus on enhancing international collaboration, information sharing, and incident response by evaluating the challenges of sharing sensitive information between responsible national and government authorities.

Research and Development Subgroup

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 Sectors (CIKR) 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/*

The Research and Development Subgroup will identify existing and planned R&D needs and priorities as they relate to industrial control systems and identify desired areas of ICS research not currently underway.

Roadmap to Secure Industrial Control Systems

The Roadmap to Secure ICS Subgroup will plan, coordinate, and develop a cross-sector roadmap to address cyber risk management within control systems environments.

Vendor Subgroup

The Vendor Subgroup will identify ways to improve information sharing between vendors, owners and operators, and other organizations involved in securing ICS. The Subgroup will create a more effective framework for cyber risk management within ICS environments.

Workforce Development Subgroup

The Workforce Development Subgroup will identify existing industrial control systems security curricula and make recommendations to enhance or create a new curriculum. The subgroup will also evaluate certification programs for control systems security professionals and work to develop an outreach plan for the control systems security workforce.

To learn more or get involved with any of these subgroups, email icsjwg@dhs.gov.

ICSJWG 2009 Annual Fall Conference & Call for Papers

The ICSJWG 2009 Fall Conference will be held November 3 – 5 2009 in Idaho Falls, ID. 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. Conference details will be posted to http://www.us-cert.gov/control_systems/icsjwg/.

The program committee is accepting abstracts for proposed presentations focused on cyber security issues impacting critical infrastructure industrial control systems. Presentations should be current, topical, informative, interactive, and address multiple stakeholders. ICSJWG will also consider proposals for panel discussions. Details about submitting abstracts for presentations or panels can be found at <https://secure.inl.gov/icsjwg-callforpapers09/>

Contact Information

If you would like to contact the ICSJWG to ask a question or inquire about participation, please send an email to 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/

ICS-CERT Email: ics-cert@dhs.gov

Phone: 1-877-776-7585

CSSP Email: cssp@dhs.gov