*Control Systems Security Program*

# INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

Critical Infrastructure and Key Resources (CIKR) support the essential functions and services that keep America operating. Some CIKR elements are so vital that an interruption in their services could have a debilitating impact on national security and economic well-being.

Although each critical infrastructure industry is vastly different, all have one thing in common--they depend on industrial control systems (ICS) to monitor, control, and safeguard their processes.

ICS, also known as Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), are essential to industry and government because they support the operation of our Nation's CIKR Sectors. As such, the Department of Homeland Security (DHS) recognizes that the protection and security of ICS is essential to the economy and security of our Nation.

## BRIDGING THE COMMUNICATIONS GAP

Within the National Cyber Security Division (NCSD) of DHS, the Control Systems Security Program (CSSP) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate knowledge sharing between the Federal government and private sector owners and operators in all CIKR sectors in an effort to reduce the risk of ICS cyber threats.

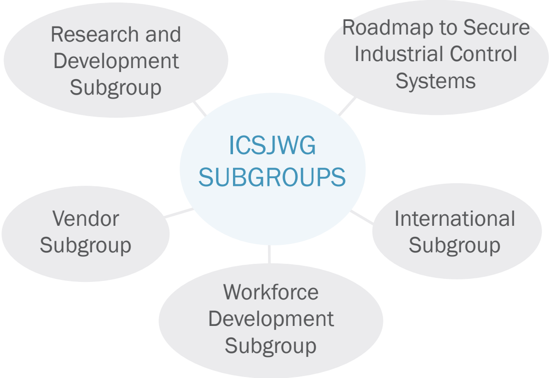
The ICSJWG operates under the National Infrastructure Protection Plan (NIPP) framework and Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The group's goal is to enhance the collaboration of ICS stakeholders by securing CIKR and accelerating the design, development, deployment, and secure operations of ICS.

The ICSJWG is a principle component of DHS's Strategy to Secure Control Systems, providing a coordinating body for sharing information and facilitating stakeholder efforts to manage cybersecurity risk.

Homeland Security

## ICSJWG SUBGROUPS

The ICSJWG members have commissioned the following five subgroups.



ICSJWG SUBGROUPS

Research and Development Subgroup

Roadmap to Secure Industrial Control Systems

Vendor Subgroup

International Subgroup

Workforce Development Subgroup

**THE INTERNATIONAL SUBGROUP** will focus on enhancing international collaboration, knowledge sharing, and incident response by evaluating the challenges of sharing sensitive information between responsible national and government authorities.

**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.

**THE ROADMAP TO SECURE ICS SUBGROUP** will maintain the Cross-Sector Roadmap to address cyber risk management within control systems environments and will coordinate its use.

**THE VENDOR SUBGROUP** will identify ways to improve information sharing between vendors, owners and operators, and other organizations involved in securing ICS.

**THE WORKFORCE DEVELOPMENT SUBGROUP** will continue to identify existing industrial control systems security curricula and make recommendations to enhance or create a new curriculum.

## INTERNATIONAL

The International Subgroup addresses the growing need for international coordination to manage cyber risk in control systems environments both domestically and abroad. Key responsibilities include:

- Preparing a comprehensive "players" manual of international Computer Emergency Response Teams (CERTs) and their organization's contact and focus information;
- Preparing a communications plan for international collaboration;
- Documenting available collaboration tools, including a gap analysis to identify needed enhancements; and
- Identifying international document handling/classification standards and performing a feasibility study to develop a common lexicon.

## RESEARCH AND DEVELOPMENT

The Research and Development Subgroup facilitates communication between ICS stakeholders and the research and development community to ensure effective focus for research and development initiatives and associated funding. Key responsibilities include:

- Documenting current and planned projects with associated details, timelines, and stakeholders involved;
- Documenting results of an ICS research and development needs assessment; and
- Preparing 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

The Roadmap to Secure ICS Subgroup creates a strategic plan to address the high-level management of cyber risk within control systems environments. The first version of the Roadmap was released in September 2011. Key responsibilities include:

- Documenting common threads for ICS challenges, priorities, and objectives across all infrastructure sectors for input to the ICS Roadmap;
- Performing a gap analysis to identify areas that need to be addressed; and
- Demonstrating a common vision and way-ahead for ICS security for all sectors.

## VENDOR

The Vendor Subgroup addresses challenges and discusses issues related to managing risk associated with control systems products and services. The Subgroup also works to identify ways to improve collaboration and information sharing between vendors, owners, operators, and other organizations involved in securing ICS. Key responsibilities include:

- Developing white papers pertinent to the ICS community, including the Vulnerability Disclosure Paper and the Cross-Vendor Position White Paper;
- Documenting stakeholder groups, challenges, and equities; and
- Preparing recommendations that address all ICS groups and areas of concern.

## WORKFORCE DEVELOPMENT

The Workforce Development Subgroup addresses challenges and priorities related to personnel awareness of cybersecurity issues within control systems environments and the development of skills for more effective cyber risk management. Key responsibilities include:

- Performing a gap analysis of control systems security workforce capabilities and development opportunities;
- Preparing a feasibility study for a control systems security certification program;
- Developing knowledge domain areas for a certification program; and
- Developing a control systems security workforce outreach plan.

## ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

**For more information,
visit www.us-cert.gov/control_systems.**