



Critical Infrastructure and Key Resources (CIKR) support the essential functions and services that underpin American society. Some CIKR elements are so vital that their destruction, incapacitation, or exploitation could have a debilitating impact on national security and economic well-being. Homeland Security Presidential Directive 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," directs the U.S. Department of Homeland Security (DHS) to produce a comprehensive, integrated national plan for CIKR protection. HSPD-7 also designates the Department of Homeland Security's (DHS) National Cyber Security Division (NCS) as a national focal point for the security of cyberspace.

Although each critical infrastructure industry is vastly different, each has one thing in common: they all depend on industrial control systems to monitor, control, and safeguard their processes.

Industrial control systems (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, DHS recognizes that protection and security of ICS is essential to the Nation's security and economy.

Bridging the Communications Gap

Within NCS, the Control Systems Security Program (CSSP) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk of cyber threats to the Nation's ICS.

The ICSJWG operates under the National Infrastructure Protection Plan (NIPP) framework and Critical Infrastructure Partnership Advisory Council (CIPAC) requirements. The group facilitates partnership between the Federal Government and private sector owners and operators in all CIKR sectors. 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 coordination group for sharing information and facilitating stakeholder efforts to manage cybersecurity risk.

ICSJWG Subgroups

The ICSJWG members have commissioned the following six subgroups.

Information Sharing

The Information Sharing Subgroup addresses 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 include:

- Documenting current information sharing mechanisms and preparing recommendations to address gaps;
- Documenting existing vulnerability reporting procedures and deficiencies;
- Preparing a recommendations guide for addressing the identified gaps, improving vulnerability disclosure, and implementing mitigation strategies; and
- Developing a clear set of reporting and incident handling guidelines.

International

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

- 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 industrial control systems stakeholders and the research and development community to ensure effective focus for research and development initiatives and associated funding. Key milestones 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. Key milestones 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
- Preparing a draft roadmap.

Vendor

The Vendor Subgroup addresses challenges and discusses issues related to managing risk associated with control systems products and services. Key milestones include:

- Documenting stakeholder groups, challenges, and equities; and
- Preparing recommendations that address all groups and areas of concerns.

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 milestones 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 DHS and NCS

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. NCS is DHS' lead agency for securing cyberspace and our Nation's cyber infrastructure.

For more information, please visit: www.dhs.gov/cyber.

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.

To learn more about the CSSP, visit www.us-cert.gov/control_systems/ or e-mail cssp@dhs.gov.

