



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 Department of Homeland Security (DHS) to produce a comprehensive, integrated national plan for CIKR protection. HSPD-7 also designates the National Cyber Security Division (NCSA) as a national focal point for the security of cyberspace.

A successful cyber attack on a control system could potentially result in physical damage, loss of life, and cascading effects that could disrupt services. As such, DHS recognizes the protection and security of control systems is essential to the Nation's overarching security and economy.

## Control Systems Security Program

To lead this effort, NCSA established the Control Systems Security Program (CSSP). The goal of the CSSP is to guide a cohesive effort between government and industry to reduce the cyber risk to industrial control systems. The CSSP provides guidance and reduces risk to CIKR control systems by:

- Leading the **Strategy to Secure Control Systems** as part of the overall mission to coordinate and lead efforts to improve control systems security in the Nation's critical infrastructures;
- Operating the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) in coordination with the United States Computer Emergency Readiness Team (US-CERT) for control systems related incidents and cybersecurity situational awareness activities;
- Maintaining a technical support center to conduct assessments of commercially available control systems and components;
- Creating informational products and tools to assist vendors and owners/operators in designing, procuring, installing, and operating control systems to mitigate risks;
- Providing strategic recommendations to the research and development community for development and testing of next-generation secure control systems;
- Assisting national and international standards organizations develop control systems cybersecurity standards;
- Managing and operating the Industrial Control Systems Joint Working Group (ICSJWG) to provide a formal mechanism to protect information and foster the coordination of activities and programs across government and private sector stakeholders; and
- Performing outreach activities and improving awareness in the control system community through training and education.



Although each of the CIKR industries is vastly different, they all have one thing in common: dependence on industrial control systems (ICS) to monitor, control, and safeguard their processes. ICS, which include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), are essential to industry and government, as these systems support the operation of our Nation's CIKR sectors. As such, the Department of Homeland Security (DHS) recognizes the protection and security of ICS is essential to the Nation's overarching security and economy.

## Protecting Systems that Control Our Infrastructure

Increasingly, control systems are transitioning from proprietary, closed systems to commercial off-the-shelf technologies connected to open networks, such as the Internet. This transition exposes control systems to the ever-present cyber risks that exist.





## CSSP Partnerships

The CSSP, in alignment with the DHS National Infrastructure Protection Plan (NIPP) partnership framework, works closely with, and coordinates efforts among, government entities, national laboratories, industry, as well as technical professionals across the control systems community. This coordination “landscape” is comprised of the many functions, stakeholders, and processes that further the implementation of technology and methods to improve control systems security. Some of the coordination groups include:

- The **Industrial Control Systems Joint Working Group** (ICSJWG) manages six subgroups to address specific issues related to international matters, research and development, workforce development, information sharing, vendor concerns, and the creation of a cross sector roadmap to secure ICS
- The **Federal Control Systems Security Working Group** works with Federal partners and the Intelligence Community to coordinate efforts to secure ICS.
- The **Industrial Control Systems Cyber Emergency Response Team** provides recognized cyber incident response and analysis capabilities, addresses the security, threat, and awareness issues unique to control systems, and provides a means to share information across all CIKR.

## CSSP Informational Products and Resources

The CSSP has created a variety of products, tools, and resources available online. Examples include control systems self-assessment software (for owners and operators to assess their control systems and recommend security improvements), control systems recommended practices, cybersecurity procurement language including specifications and guidance, vulnerability notes, training and Web-based courses, links to industry standards and references, and other valuable resources and information.

## Reporting Control Systems Cyber Incidents and Vulnerabilities

CSSP encourages 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/>. You can also submit reports via one of the following methods:

Phone: 1-888-282-0870  
ICS related cyber activity: [ics-cert@dhs.gov](mailto:ics-cert@dhs.gov)  
General cyber activity: [soc@us-cert.gov](mailto:soc@us-cert.gov)

For general program questions or comments, please contact [cssp@dhs.gov](mailto:cssp@dhs.gov).

### About DHS and NCSD

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. NCSD is DHS’ lead agency for securing cyberspace and our Nation’s cyber infrastructure.

For more information, please visit: [www.dhs.gov/cyber](http://www.dhs.gov/cyber).

