Our nation depends on the continuous and reliable performance of a vast and interconnected critical infrastructure to sustain our way of life. This infrastructure, the majority of which is owned by the private sector, is comprised of critical infrastructures and key resources (CI/KR), such as Energy, Chemical, Banking and Finance, Dams, Water Treatment Systems, Postal and Shipping, Information Technology Telecommunications, Commercial Nuclear Reactors, and many more.

Resilient, Secure, Reliable Infrastructure

Although each of the critical infrastructure industries is vastly different, they all have one thing in common: they are dependent on control systems to monitor, control, and safeguard their processes.

Industrial control systems (ICS), which may also be known as Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS), are essential to industry and government alike, as these systems support the operation of our nation's critical infrastructure and key resources.

Protecting the Systems that Control Our Infrastructure

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

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, the U.S. Department of Homeland Security (DHS) recognizes that 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, the Department's National Cyber Security Division (NCSD) 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:

- 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.
- 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.
- Performing outreach activities and improving awareness in the control system community through training and education.
- Creating informational products and tools to assist vendors and owners/operators in designing, procuring, installing, maintaining, and operating controls 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 in the development of control systems cybersecurity standards.

CSSP Partnerships

The CSSP, in alignment with the DHS National Infrastructure Protection Plan (NIPP), 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:

- ***Industrial Control Systems Joint Working Group*** - Operated by CSSP, this group provides a formal mechanism to protect information and foster the coordination of activities and programs across government and private sector stakeholders.
- ***Federal Control Systems Security Working Group*** - CSSP works with this group to coordinate federal efforts.
- ***Working Groups Chartered by the ICSJWG*** - Various control systems working groups have evolved out of the ICSJWG to address the needs of different communities of interest. This includes stakeholders within the vendor community and the research and development community who are focused on cybersecurity issues facing control systems infrastructure.
- ***The International Community*** - CSSP works with various international partners and working groups to facilitate information sharing and rapid adoption of international recommended practices.

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.

To access this material or learn more about control systems related cyber vulnerabilities, training, standards and references, visit http://www.us-cert.gov/control_systems.

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
General cyber activity: soc@us-cert.gov

For general program questions or comments, please contact cssp@dhs.gov .

About DHS and NCSD

The Department of Homeland Security (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. The National Cyber Security Division (NCSD) leads the DHS efforts to secure cyberspace and our Nation's cyber assets and networks.