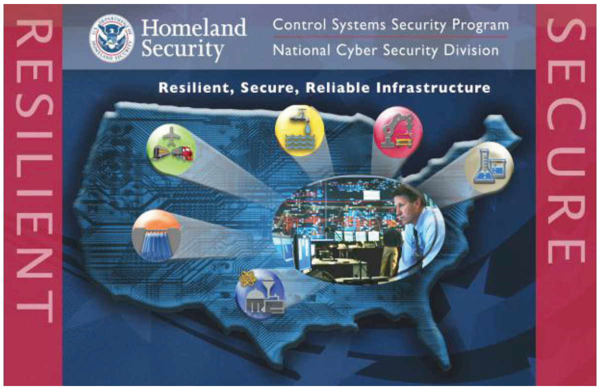
# Strategy for Securing Control Systems

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, includes sectors such as, Energy, Chemical, Banking and Finance, Water Treatment Systems, Postal and Shipping, Information Technology, Telecommunications, Commercial Nuclear Reactors, and Transportation.




Although each Critical Infrastructure and Key Resource (CIKR) sector is vastly different, they all share one thing in common--they are all dependent on industrial control systems to monitor, control, and safeguard their critical processes.

Industrial control systems (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 alike, as these systems support the operation of our nation's CIKR sectors. As such, the U.S. Department of Homeland Security (DHS) has recognized that the protection and security of ICS is essential to the Nation's overarching security and economy.

## One Common Vision

DHS's National Cybersecurity Division (NCSD) created the Strategy for Securing Control Systems as part of the overall mission to coordinate and lead efforts to improve control systems security in the nation's critical infrastructures.

The primary goal of the Strategy is to build a long-term common vision where effective risk management of ICS security can be realized through successful coordination efforts between public and private CIKR stakeholders. Implementing the Strategy will create a common vision with respect to participation, information sharing, coalition building, and leadership activities. Its implementation will improve coordination among relevant ICS stakeholders within government and private industry, thereby reducing cybersecurity risks to all CIKR Sectors.

## The Coordination Challenge

By participating in and supporting this Strategy, partnering organizations develop a shared vision that will benefit both public and private sector stakeholders. The "coordination landscape" is defined by the Strategy and includes specific activities and initiatives that are enhancing the nation's security posture.

Effectively and efficiently securing the nation's critical infrastructure ICS from cyber attack requires extensive coordination and participation of both public and private sector security entities. Government and private sector partners bring a wide range of core competencies and perspectives that add value to the partnership and enable each partner to fulfill its cybersecurity mission. The benefits of implementing this coordination strategy include:

- Providing opportunities to incorporate specific ICS activities into federal, state, and local security program design and investment.
- Managing risk through timely and accurate dissemination of information on CIKR sector threats and vulnerabilities, recommended practices, assessment methodologies, research and development, and other critical information.
- Improving information sharing between stakeholders through relationship building and establishing trust.
- Improving ICS communication networks resulting in greater impact and reach of security partner efforts to government agencies, the public, and others.
- Improving accuracy and relevance to the type of environment (e.g., voluntary, regulatory) through which sector security is promulgated.
- Addressing ICS security gaps and avoiding duplication of efforts.

Homeland Security

# Strategy for Securing Control Systems

## The ICSJWG and ICS-CERT

The overarching Strategy has two principal operational components:

1. The Industrial Control Systems Joint Working Group **(ICSJWG)**; and
2. The Industrial Control Systems Cyber Emergency Response Team **(ICS-CERT).**

These two components of the Strategy are essential elements to achieving overall coordination within the National Infrastructure Protection Plan (NIPP) partnership framework.

The **ICSJWG** provides broad coordination of control systems security activities among stakeholders across the 18 CIKR Sectors. The ICSJWG manages 6 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 **ICS-CERT**, operated by the DHS Control Systems Security Program (CSSP), 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 Sectors.

These key components of the Strategy provide DHS with the mechanisms for coordinating partnerships and stakeholder efforts to manage cybersecurity risk effectively. Through these two components, DHS will significantly advance its mission to secure cyberspace and America's cyber assets, including industrial control systems security within critical infrastructure and key resources.

## Obtaining Additional Information

To learn more about the Strategy to Secure Control Systems or the Control Systems Security Program, visit: http://www.us-cert.gov/control_systems/ or email: cssp@dhs.gov.

## Reporting Control Systems Cyber Incidents and Vulnerabilities

DHS and CSSP encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online forms are available at: https://forms.us-cert.gov/report/. You can also submit reports via one of the following methods:

- Phone: (888) 282-0870
- ICS Related Cyber Activity: ics-cert@dhs.gov.
- General Cyber Activity: soc@us-cert.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.