



STRATEGY FOR SECURING CONTROL SYSTEMS

Our Nation depends on the continuous and reliable performance of a vast and interconnected critical infrastructure (CI) 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, Postal and Shipping, Information Technology, Telecommunications, Nuclear, and Transportation.

Although each CI sector is vastly different, they share one thing in common—they are all dependent on industrial control systems (ICS) to monitor, control, and safeguard their critical 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 alike, as these systems support the operation of our nation's CI sectors.

As such, the U.S. Department of Homeland Security (DHS) recognizes that the protection and security of ICS is essential to the nation's overarching security and economy.

ONE COMMON VISION

DHS' Office of Cybersecurity and Communications (CS&C) created the Strategy for Security Control Systems as part of the overall mission to coordinate and lead efforts to improve control systems security in the nation's CI.

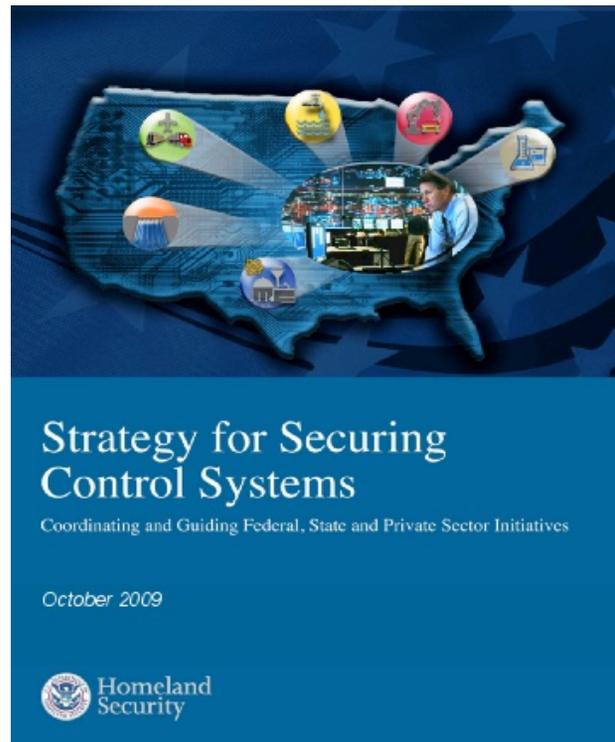
The primary goal of the Strategy is to build a long-term common vision where effective risk management of ICS security can be realized through successful coordination efforts between public and private CI stakeholders.

Implementation of the Strategy creates a common vision with respect to participation, information sharing, coalition building, and leadership activities. Its implementation also

improves coordination among relevant ICS stakeholders within government and private industry, thereby reducing cybersecurity risks to all CI sectors.

THE COORDINATION CHALLENGE

By participating in and supporting this Strategy, partnering organizations develop a shared vision that 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 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 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 CI 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.

THE ICSJWG AND ICS-CERT

The overarching Strategy has two principal operational components:

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

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

ICS-CERT works to reduce risks within and across all CI sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts across all ICS stakeholders.

The ICSJWG is the public-private-partnership vehicle of ICS-CERT and provides an opportunity for communicating and partnering across all CI sectors, between federal agencies and departments, as well as private asset owner/operators of ICS.

The key components of the Strategy provide DHS with stakeholder efforts to manage cybersecurity risk effectively. Through these two components, DHS significantly advances its mission to secure cyberspace and America's cyber assets, including ICS security within CI.

About ICS-CERT

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

<https://ics-cert.us-cert.gov>

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

<http://www.dhs.gov/national-cybersecurity-communications-integration-center>