Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) 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. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

IMPROVING THE NATION'S CYBERSECURITY POSTURE

As a functional component of the NCCIC, the ICS-CERT is a key component of DHS's Strategy for Securing Control Systems. The primary goal of the strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts. ICS-CERT leads this effort by:

- Responding to and analyzing control systems related incidents
- Conducting vulnerability, malware, and digital media analysis
- Providing onsite incident response services
- Providing situational awareness in the form of actionable intelligence
- Coordinating the responsible disclosure of vulnerabilities and associated mitigations
- Sharing and coordinating vulnerability information and threat analysis through information products and alerts.

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.

ONSITE INCIDENT RESPONSE

The ICS-CERT also provides onsite incident response, free of charge, to organizations that require immediate investigation and resolve in responding to a cyber attack. Upon notification of a cyber incident, ICS-CERT will perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, ICS-CERT can deploy a team to meet with the affected organization to review network topology, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow on analysis. ICS-CERT is able to provide mitigation strategies and assist asset owners/operators in restoring service and provide recommendations for improving overall network and control systems security.

ADVANCED ANALYTICAL LABORATORY

The Advanced Analytical Laboratory (AAL) incident response activities are a key service offering from ICS-CERT. The AAL provides analysis of malware threats to control system environments, as well as offering asset owners onsite assistance and remote analysis to support discovery, forensics analysis, and recovery efforts.

CYBERSECURITY EVALUATION TOOL

Cybersecurity Evaluation Tool (CSET) is a desktop software tool that enables users to self-assess their network and ICS security practices against recognized industry and government standards, guidelines, and recommended practices. A complete CSET assessment report provides a prioritized list of options for improving the cybersecurity posture of an organization's ICS or enterprise network, and identifies what is needed to achieve the desired level of security relative to the specific standard(s) selected. Download the CSET at https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET.

SITE ASSISTANCE AND EVALUATIONS

The ICS-CERT provides site assistance and evaluations to strengthen the Nation's ICS security posture for critical infrastructure control systems owners, operators, and manufacturers. ICS-CERT also provides incident handling and vulnerability coordination activities through onsite assessments, analysis, and mitigation techniques to counter cybersecurity exploits and intrusions.

OUTREACH AND TRAINING

ICS-CERT performs outreach activities to help critical infrastructure sectors understand the cybersecurity risks associated with ICS, and assists the control systems community to improve their cybersecurity preparedness through training and education. For information on ICS-CERT training courses visit https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT.

INDUSTRIAL CONTROL SYSTEMS JOINT WORKING GROUP

The Industrial Control Systems Joint Working Group (ICSJWG) is a collaborative and coordinating body formed under the Critical Infrastructure Partnership Advisory Council Framework. The ICSJWG facilitates partnerships between the Federal Government and private sector owners and operators in all critical infrastructure (CI) sectors. The goal of the ICSJWG is to enhance collaboration with ICS stakeholders toward securing CI by accelerating the design, development, and deployment of secure ICS.

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