About the Industrial Control Systems Cyber Emergency Response Team

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS 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; and
- sharing and coordinating vulnerability information and threat analysis through information products and alerts.

ICS-CERT coordinates control systems-related security incidents and information sharing with Federal, State, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

As a functional component of the NCCIC, ICS-CERT provides focused operational capabilities for defense of control system environments against emerging cyber threats.

ICS-CERT provides efficient coordination of control-systems-related security incidents and information sharing with federal, state, and local agencies and organizations, the Intelligence Community, private sector constituents including vendors, owners, and operators, and international and private sector computer security incident response teams (CSIRTs). The focus on control systems cybersecurity provides a direct path for coordination of activities for all members of the stakeholder community.

Download the NCCIC/ICS-CERT Fact Sheet

Download the NCCIC/ICS-CERT Incident Handling Brochure

Onsite Incident Response

ICS-CERT provides onsite incident response, free of charge, to organizations that require immediate analysis and mitigations in response 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 an onsite support 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 can provide mitigation strategies and assist asset owners/operators with recommendations for improving overall network and control systems security.

Programs, Activities, and Partnerships

Advanced Analytic Lab. ICS-CERT operates an advanced analytic lab (AAL) that performs digital media and malware analysis on samples from infected systems. The lab also hosts a representative sample of vendor equipment onsite to give analysts testing capabilities of malware in control system environments. The availability of onsite equipment and software allows ICS-CERT to assess the possible effects of malicious software and consequences a vulnerability may have on critical infrastructure.

Partnerships. ICS-CERT is a component of the National Cybersecurity and Communications Integration Center (NCCIC), bringing industrial control systems security technical and response capabilities to the partnership. The work is performed in conjunction with the NCCIC and furthers the overall mission to coordinate defense against and response to cyber attacks across the nation.

ICS-CERT works to reduce risk within and across all critical infrastructure sectors by coordinating efforts among federal, state, local and tribal governments, as well as control systems owners, operators, and vendors. In addition, ICS-CERT collaborates with international and private sector CERTs to share control systems related security incidents and mitigation measures.

ICS-CERT participates with many working groups including the Industrial Control Systems Joint Working Group and the Federal Control Systems Security Working Group. These trusted relationships are leveraged to increase and improve information sharing with the CIKR asset owner/operators and vendor community.

ICS-CERT also brings control systems and cybersecurity technical expertise and incident response capabilities to its partnership with the United States Computer Emergency Readiness Team (US-CERT). Both entities operate side-by-side within the NCCIC to provide a single source of support to critical infrastructure stakeholders.