Homeland Security

ICS-CERT

Industrial Control Systems Cyber Emergency Response Team

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 national assets and key resources such as Energy, Chemical, Banking and Finance, Dams, Water Treatment Systems, Postal and Shipping, Information Technology, Telecommunications, Transportation, Commercial Nuclear Reactors, and many more.

With cyber threats to these computer systems on the rise, the U.S. Department of Homeland Security (DHS) created the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to provide industrial control system stakeholders with situational awareness and analytical support to effectively manage risks.

ICS-CERT Works to Protect America's Control Systems

The DHS Control Systems Security Program (CSSP) manages and operates the ICS-CERT in coordination with the US Computer Emergency Readiness Team (US-CERT) to provide focused operational capabilities for defense of control system environments against emerging cyber threats.

The ICS-CERT is a key component of the *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. The ICS-CERT leads this effort by:

- Responding to and analyzing control systems related incidents
- Conducting vulnerability and malware analysis

- Providing onsite support for forensic investigations
- 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

The ICS-CERT provides more efficient coordination of 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 cyber security provides a direct path for coordination of activities among all members of the stakeholder community.

Malware Lab Provides Unique Capability

The ICS-CERT also operates a malware lab, which provides testing capabilities to analyze vulnerabilities and malware threats to control system environments. The lab is able to configure representative samples of control system equipment commonly used within critical infrastructure to support this testing and analysis capability.

ICS-CERT Partners With Others to Protect

The ICS-CERT collaborates with the US-CERT, bringing technical expertise and incident response capabilities related to industrial control systems security to the partnership. The work is performed in conjunction with US-CERT and supports their overall mission to coordinate defense against and response to cyber attacks across the nation. Both entities operate side-by-side within the National Cybersecurity and Communications Integration Center to provide a single source of support to critical infrastructure stakeholders.

The ICS-CERT works to reduce risks 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.

The ICS-CERT collaborates with international and private sector CERTs to share control systems related security incidents and mitigation measures.

The 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 critical infrastructure and key resource asset owner/operators and the vendor community.

About DHS:

DHS is responsible for safeguarding our nation’s critical infrastructure from physical and cyber threats that affect our national security, public safety, and economic prosperity. The ICS-CERT is operated by the Control Systems Security Program under the National Cyber Security Division (NCSD). NCSD works collaboratively with public, private. and international entities to secure cyberspace and America’s cyber assets.

To 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 and ICS-CERT encourage 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:

ICS-CERT Watch Floor: 1-877-776-7585

ICS related cyber activity: ics-cert@dhs.gov

General cyber activity: soc@us-cert.gov

US-CERT Phone: 1-888-282-0870