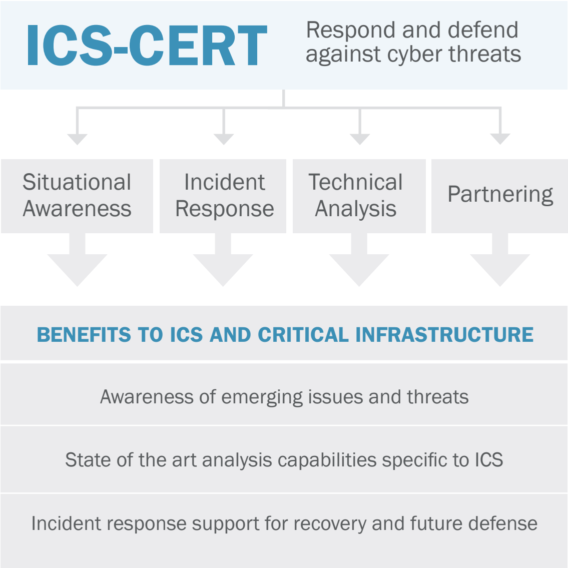
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is the operational arm of the Control Systems Security Program (CSSP). The U.S. Department of Homeland Security's (DHS) National Cyber Security Division (NCSD) created both ICS-CERT and CSSP to combat rising cyber threats to critical infrastructure. ICS-CERT provides industrial control systems (ICS) stakeholders with incident response services, vulnerability coordination, situational awareness, and analytical support to effectively manage cyber threats and reduce risks.



ICS-CERT Respond and defend against cyber threats

Situational Awareness

Incident Response

Technical Analysis

Partnering

BENEFITS TO ICS AND CRITICAL INFRASTRUCTURE

Awareness of emerging issues and threats

State of the art analysis capabilities specific to ICS

Incident response support for recovery and future defense

PROTECTING AMERICA'S CONTROL SYSTEMS

ICS-CERT's mission is to reduce risk to critical infrastructure industrial control systems by providing incident response and tactical mitigation information to protect against emerging cyber threats. ICS-CERT accomplishes this by engaging with both private and public partners to share and fuse information in order to comprehensively assess the threat landscape and provide mitigations to the community at large. 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.

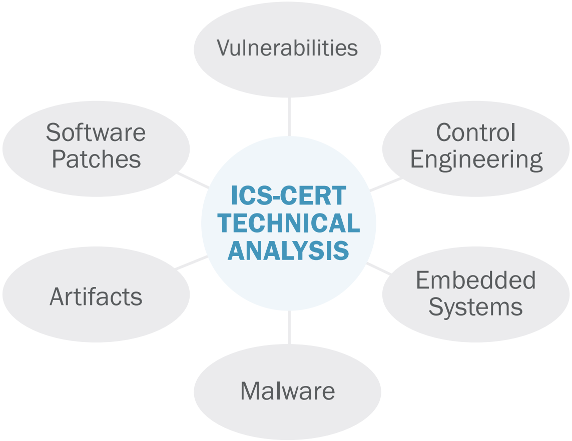
ICS-CERT is a key component of DHS's Strategy for Securing Control Systems. The primary goal of the Strategy is to build a long-term common vision where effective risk management of control systems security can be realized through successful coordination efforts.

Homeland Security

UNIQUE CAPABILITIES

ICS-CERT operates an Advanced Analytics Lab (AAL) to analyze vulnerabilities, perform digital media and log file analysis, and analyze malware threats to control systems environments. The AAL provides unique capabilities and technical expertise in both industrial control systems and cybersecurity. These capabilities include the ability to configure representative test environments of control system equipment commonly used within critical infrastructure to support this testing and analysis capability.

ICS-CERT leverages these capabilities to provide analytic services to companies requesting support in response to an incident. ICS-CERT is able to analyze hard drives, log files, malware, and other artifacts and provide detailed indicators and analysis reports to assist organizations in detecting and mitigating malicious activity.



PARTNERSHIPS

ICS-CERT works to reduce risks within and across all critical infrastructure sectors. In particular, ICS-CERT partners with law enforcement agencies and the intelligence community, coordinates efforts among federal, state, local, and tribal governments, and works with control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector CERTs to share control systems related security incidents and mitigation measures.

ICS-CERT also operates side-by-side within the National Cybersecurity and Communications Integration Center (NCCIC) with a variety of partners such as the United States Computer Emergency Readiness Team (US-CERT), to provide a single source of support to respond to cyber threats against industrial control systems.

ICS-CERT participates with many working groups including the Industrial Control Systems Joint Working Group and the Cross-Sector Cyber Security Working Group. These trusted relationships are leveraged to increase and improve information sharing with critical infrastructure and key resource asset owners and operators as well as the vendor community.

RESOURCES FOR ASSET OWNERS

ICS-CERT posts recommended practices guidelines, whitepapers, and alerts and advisories about ICS threats and vulnerabilities to the web at **www.ics-cert.org** and shares more sensitive information through the US-CERT secure portal. Asset owners can request access to the Control Systems Center compartment of the US-CERT portal by emailing **ics-cert@dhs.gov.**

REPORTING CYBER INCIDENTS AND EVENTS

CSSP and ICS-CERT encourage you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Reports can be submitted to ICS-CERT via one of the following methods:

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

ICS Related Cyber Activity: ics-cert@dhs.gov

For general program questions or comments contact cssp@dhs.gov **or visit** www.us-cert.gov/control_systems.

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. The National Cyber Security Division (NCSD) is DHS' lead agency for securing cyberspace and our Nation's cyber infrastructure. ICS-CERT is operated by the CSSP under NCSD.

For more information visit www.dhs.gov/cyber.