Information For

Control System Users

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats.

About Us

US-CERT is part of DHS' National Cybersecurity and Communications Integration Center (NCCIC).

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the Nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity—collaborative, agile, and responsive in a dynamic and complex environment.

Frequently Asked Questions

Where can I find current cybersecurity information?

You can subscribe to US-CERT's mailing lists and feeds. US-CERT distributes vulnerability and threat information through its National Cyber Awareness System (NCAS), and operates a Vulnerability Notes Database to provide technical descriptions of system vulnerabilities.

How does US-CERT fulfill its mission?

Through its 24x7 operations center, US-CERT accepts, triages, and collaboratively responds to incidents; provides technical assistance to information system operators; and disseminates timely notifications regarding current and potential security threats and vulnerabilities.

What is US-CERT's relationship to DHS?

US-CERT is the 24-hour operational arm of the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC).

How do I report an incident to US-CERT?

Click here to report a cyber incident. Click here to report a software vulnerability.

What is the relationship between US-CERT and other groups with "CERT" in their name?

Worldwide, there are more than 250 organizations that use the name "CERT" or a similar name and deal with cybersecurity response. US-CERT is independent of these groups, though we may coordinate with them on security incidents.

How does US-CERT protect sensitive information?

US-CERT leverages the Protected Critical Infrastructure Information (PCII) Program to prevent inappropriate disclosure of proprietary information or other sensitive data. Established in response to the Critical Infrastructure Information Act of 2002 (CII Act), the PCII Program enables members of the private sector to voluntarily submit confidential information regarding the nation's critical infrastructure to DHS with the assurance that the information will be protected from public disclosure. More details about how information can be protected under the CII Act can be found on the Department of Homeland Security website.

Who are US-CERT's partners?

US-CERT partners with private sector critical infrastructure owners and operators, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local partners, and domestic and international organizations to enhance the Nation's cybersecurity posture.

Press Releases