Homeland Security

Cyber Information Sharing
with DHS' CERTs

GUIDELINES

PRODUCT AVAILABILITY

SECURE PORTAL COMMUNICATIONS

DISTRIBUTING INFORMATION

ADDITIONAL RESOURCES

WORKING GROUPS

A CERT performs functions required in an emergency, and encourages effective response practices community-wide through outreach and education. DHS has two Internet security-focused CERTs: ICS-CERT and US-CERT.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) shares information about control systems-related security incidents and mitigation measures (*https://ics-cert.us-cert.gov*). The United States Computer Emergency Readiness Team (US-CERT) handles computer security incidents of all kinds (*https://www.us-cert.gov*).

GUIDELINES

How to Report an Incident:

The US-CERT Incident Reporting System provides a web-enabled means to report computer security incidents to the U.S. Department of Homeland Security. Reports are routed from one centralized interface to the appropriate team to handle. *https://www.us-cert.gov/forms/report*

Federal agencies must report certain computer security incidents, all other reporting is voluntary. Agency requirements are publically available: *https://www.us-cert.gov/incident-notification-guidelines*

Control systems operators can report incidents, or threats that are targeted in nature, directly to ICS-CERT by emailing *ics-cert@hq.dhs.gov*.

A few benefits of voluntary reporting:

- **We can help.** Upon request, ICS-CERT and/or US-CERT may provide remote or on-site response support to entities affected by significant incidents.
- **Better analysis.** Often, constituents don't require hands-on support to resolve a given incident, but providing us awareness of it improves our ability to assess impact and recoverability on a broader scale, which can help to prevent recurrences.
- **Awareness raising.** We use information reported to us to develop and publish workarounds and mitigations that may prevent negative impacts to companies and end users facing similar threats.

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 US-CERT

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. *https://www.us-cert.gov*

PRODUCT AVAILIABILTIY

Products:

- **Advisories and Alerts** offer timely information about current security issues, vulnerabilities and exploits.
- **Bulletins** provide weekly summaries of new computer security vulnerabilities; patch information is provided when available.
- **Current Activity** updates offer up-to-date information about high-impact types of security activity affecting the community at large.
- **Monitor** newsletters offer awareness of ICS-CERT's recent incident response activities, products released, and upcoming events.
- **Tips** provide advice to the general public about common security issues.

All products are available through our public websites *https://www.us-cert.gov/* and *https://ics-cert.us-cert.gov/*.

How to subscribe:

Subscriptions to US-CERT's products, designed for all computer security users and practitioners, can be found on *https://www.us-cert.gov/ncas*. Subscriptions to information developed for and about control systems users can be found *https://ics-cert.us-cert.gov/ICS-CERT-Feeds*.

RSS Feeds are also available:

- ICS-CERT RSS feed link: *https://ics-cert.us-cert.gov/xml/rss.xml*
- US-CERT RSS feed link: *https://www.us-cert.gov/ncas/current-activity.xml*

SECURE PORTAL COMMUNICATIONS

Web-based Collaborative System

Practitioners can subscribe to a web-based collaborative system to exchange sensitive cybersecurity information among government and private sector members. ICS-CERT and US-CERT regularly publish a variety of products to the portal library.

US-CERT shares cyber threat indicators and advisory information with computer network defense professionals. Contact *info@us-cert.gov* for additional information.

ICS-CERT shares information specific to control systems threats. Contact *ics-cert@hq.dhs.gov* for additional information.

DISTRIBUTING INFORMATION

TLP

The computer security CERT community relies on the Traffic Light Protocol (TLP) to ensure that sensitive information is shared with the correct audience. TLP employs four colors to indicate different degrees of sensitivity and corresponding sharing considerations that should be applied by information recipients. The TLP matrix and list of frequently asked questions are available at *https://www.us-cert.gov/tlp*. There is no barrier to adopting this practice within your organization.

WORKING GROUPS

ICSJWG

The Industrial Control Systems Joint Working Group is a principle component of DHS's Strategy to Secure Control Systems, providing a coordinating body for sharing information and facilitating stakeholder efforts to manage cybersecurity risk. The learn more, visit: *https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG.*

ADDITIONAL RESOURCES

Advanced Analysis Laboratory

The Advanced Analytical Laboratory (AAL) provides research and analysis capabilities in support of the incident response, assessment, and vulnerability coordination activities of ICS-CERT. The AAL's expert cybersecurity researchers perform forensic analysis on digital media, reverse engineer malware, and respond to cyber incidents.

Advanced Malware Analysis

The Advanced Malware Analysis Center provides US-CERT with the capability to collect, analyze, and exchange malware information 24 hours a day. Malware artifacts can be submitted for analysis electronically at *https://malware.us-cert.gov/MalwareSubmission/pages/submission.jsf*

Phishing and Vulnerability Reports

Phishing - Report Phishing to *Phishing-Report@us-cert.gov*. Phishing-related email messages and website locations are collected in order to help people avoid becoming victims of phishing scams.

Vulnerabilities - The CERT Coordination Center performs vulnerability coordination and disclosure in support of the U.S. Government. Report vulnerabilities online at *https://forms.cert.org/VulReport/*.