



The Department of Homeland Security is responsible for protecting our Nation's critical infrastructure from physical and cyber threats. Cyberspace has integrated once distinct information infrastructures, including our business and government operations, emergency preparedness communications, and critical digital and process control systems and infrastructures. Protection of these systems is essential to the resilience and reliability of the Nation's critical infrastructures and key resources and, therefore, to our economic and national security.

US-CERT Protects America's Internet Infrastructure

The Department's National Cyber Security Division created the United States Computer Emergency Readiness Team (US-CERT) in September 2003 to protect the Nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

US-CERT collaborates with Federal agencies, the private sector, the research community, state, local, and tribal governments, and international entities. Through coordination with various national security incident response centers responding to incidents on both classified and unclassified systems and related analysis, US-CERT disseminates reasoned and actionable cyber security information to the public.

To protect America's cyberspace, US-CERT:

- Operates a 24x7 Security Operations Center.
- Administers the National Cyber Alert System to disseminate important cyber security warnings and alerts.
- Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities.
- Coordinates with law enforcement and the intelligence community.
- Provides the general public with cyber alerts and information (available at www.us-cert.gov).
- Provides agencies with access to comprehensive digital media analysis capabilities.
- Conducts malware analytic and recovery support for government agencies.
- Offers fused, current, and predictive cyber analysis based on situational reporting.
- Disseminates actionable situational awareness reports on emerging cyber threats and vulnerabilities.

- Provides on-site incident response capabilities to federal and state agencies.
- Facilitates information sharing efforts aimed at improving the Nation's cyber security posture.
- Develops and participates in regional, national, and international exercises.
- Collaborates with domestic and international computer security incident response teams.

Building Success through Relationships

US-CERT is focused on expanding its operational outreach through partnerships with private sector security vendors, academia, Federal agencies, Information Sharing and Analysis Centers (ISACs), state, local, and tribal governments, and international organizations. US-CERT participates in various information sharing venues, including the ISACs and corporate computer security incident response teams.

US-CERT Programs and Initiatives

US-CERT has established several important components that foster and facilitate information sharing and collaboration on cyber security issues among government, industry, academia, and international entities.

Examples of US-CERT collaboration efforts include:

- **US-CERT Website** – Provides government, private sector, and the public with information needed to protect information systems and infrastructures. The website includes information on current cyber activity, vulnerabilities, recent and archived alerts, events, resources, and security publications.
- **National Cyber Alert System (NCAS)** – Available via the US-CERT website, the NCAS delivers targeted, timely, and actionable information about cyber security topics and threats to users of all technical levels.
- **National Cyber Response Coordination Group (NCRCG)** – Established in partnership with the Department of Defense and the Department of Justice, NCRCG serves as the Federal Government's principal interagency mechanism to facilitate coordination of efforts to respond to and recover from cyber incidents of national significance.
- **US-CERT Secure Portal** – Provides a secure, web-based collaborative system to share sensitive cyber-related information with government and industry partners.
- **Government Forum of Incident Response and Security Teams (GFIRST)** – A community of more than 50



incident response teams from various Federal agencies working together to secure the federal government.

- **Internet Health Service** – Provides information about Internet activity to Federal government agencies through the GFIRST community.

Participation is Key to Improving Cyber Security

You can be an informed citizen by signing up to receive free alerts and important security information. There are products available for various technical levels and needs. These include:

- **Current Activity** – Notifies users of the most frequent, high-impact types of security incidents reported to US-CERT.
- **Technical Cyber Security Alerts** – Provide information about current security issues, vulnerabilities, and exploits.
- **Cyber Security Bulletins** – Summarize information that has been published regarding new vulnerabilities.
- **Cyber Security Alerts** – Alert non-technical readers to security issues that affect the general public.
- **Cyber Security Tips** – Provide information and advice for non-technical readers about common security topics.

Visit <http://www.us-cert.gov/cas/signup.html> to subscribe or learn more.

Report Cyber Incidents, Vulnerabilities, and Phishing Scams

US-CERT encourages you to report any suspicious activity, including cyber security incidents, possible malicious code, vulnerabilities, and phishing related scams. Reporting forms can be found on our homepage at www.us-cert.gov.

You can also submit cyber threats, incidents, and vulnerabilities via the following methods:

Phone: 1-888-282-0870

Fax: 703-235-5965

E-mail (in the clear and encrypted): soc@us-cert.gov

Location to obtain the Public Key:

<http://www.us-cert.gov/pgp/soc.asc>

Obtaining Additional Information

To learn more about US-CERT, visit:

www.us-cert.gov

or contact:

info@us-cert.gov