Homeland Security

US-CERT

United States Computer Emergency Readiness Team

DHS Cyber Security

The Department of Homeland Security is responsible for protecting our Nation's critical infrastructure from physical and cyber threats. Cyberspace has united once distinct information infrastructures, including our business and government operations, our emergency preparedness communications, and our 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 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, private sector, the research community, state and local governments, and international entities. By analyzing incidents reported by these entities and coordinating with national security incident response centers responding to incidents on both classified and unclassified systems, US-CERT disseminates reasoned and actionable cyber security information to the public.

To protect America's cyberspace, US-CERT:

- Maintains 24x7 Secure Operations Center.
- Established a public website (**www.us-cert.gov**) to provide the general public with cyber related information.
- Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities.
- Develops and participates in regional, national, and international level exercises.
- Supports forensic investigations with recursive analysis on artifacts.
- Provides malware analytic and recovery support for government agencies.
- Provides behavior techniques for dynamic and static analysis.
- Manages the malicious code submission and collection program.
- Disseminates emerging cyber threat warnings.
- Administers the National Cyber Alert System to disseminate cyber security information to all Americans.
- Provides fused, current, and predictive cyber analysis based on situational reporting.
- Provides on-site incident response capabilities to federal and state agencies.
- Supports ongoing federal law enforcement investigations.
- Coordinates federal programs of computer emergency response team and Chief Information Security Officer (CISO) peer groups for sharing incident information, best practices, and other cyber security information.
- Collaborates with domestic and international computer security incident response teams.

Building Success through Relationships

US-CERT is expanding its operations through partnerships with the private sector security vendors, academia, federal agencies, Information Sharing and Analysis Centers (ISACs), state and local governments, and domestic and international organizations. US-CERT participates in various information sharing venues, including leveraging the ISACs and engaging with corporate computer security incident response teams.

US-CERT plays an integral role in assisting in the development of regional programs, such as the South East Cyber Anti-Terrorism & Security (SECATS) located in the Gulf Coast, and the Puget Sound Partnership for Cyber Security located in the Pacific Northwest. These regional efforts made up of government, private, state, and local entities, were developed by the stakeholders as an information sharing mechanism.

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 current collaboration efforts include:

- **US-CERT Website** – Provides government, private sector, and the public with information needed to improve its ability to protect information systems and infrastructures. The website includes information on current activity, events, resources, publications, and affiliates.
- **National Cyber Alert System** – Delivers targeted, timely, and actionable information to Americans, educating them on how to secure their own computer systems.
- **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 Portal** – Provides a secure web-based collaborative system to share sensitive cyber-related information with government and industry members.
- **Government Forum of Incident Response Security Teams (GFIRST)** – A community of more than 50 incident response teams from various federal agencies working together to secure the federal government.
- **US-CERT Einstein Program** – Automated process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our Nation's cyber situational awareness.
- **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 cyber security information. Register on the US-CERT website at:
http://www.us-cert.gov/cas/signup.html

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 to:

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 or contact:
www.us-cert.gov
info@us-cert.gov

Cyber security is a shared responsibility. Working together, we can secure America's cyberspace.