National Cybersecurity and Communications Integration Center

Information sharing is a key part of the Department of Homeland Security's (DHS) mission to create shared situational awareness of malicious cyber activity. Cyberspace has united once distinct information structures, 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 infrastructure and key resources; therefore, to our economic and national security. DHS's National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

NCCIC Overview

The NCCIC shares information among public and private sector partners to build awareness of vulnerabilities, incidents, and mitigations. Cyber and industrial control systems users can subscribe to information products, feeds, and services at no cost.

- US-CERT Information Products
- ICS-CERT Information Products
- Report an Incident

NCCIC Vision

The NCCIC vision is a secure and resilient cyber and communications infrastructure that supports homeland security, a vibrant economy, and the health and safety of the American people. In striving to achieve this vision, the NCCIC will:

- Focus on proactively coordinating the prevention and mitigation of those cyber and telecommunications threats that pose the greatest risk to the nation.
- Pursue whole-of-nation operational integration by broadening and deepening engagement with its partners through information sharing to manage threats, vulnerabilities, and incidents.
- Break down the technological and institutional barriers that impede collaborative information exchange, situational awareness, and understanding of threats and their impact.
- Maintain a sustained readiness to respond immediately and effectively to all cyber and telecommunications incidents of national security.
- Serve stakeholders as a national center of excellence and expertise for cyber and telecommunications security issues.
- Protect the privacy and constitutional rights of the American people in the conduct of its mission.

NCCIC Mission

The NCCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks. This mission defines the NCCIC's specific contribution to achieving its vision. To execute its mission effectively, the NCCIC will focus on three core strategic priorities and associated operational objectives. The NCCIC will implement this strategy by expanding and attaining the capabilities, products, and services required to meet each of its strategic priorities over the next five years. Many of these activities will be coordinated, developed, and executed collaboratively with the NCCIC's operational partners to the benefit of the entire community of cyber and communications stakeholders.

NCCIC Branches

The NCCIC is comprised of four branches:

- NCCIC Operations and Integration (NO&I);

- United States Computer Emergency Readiness Team (US-CERT);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT); and
- National Coordinating Center for Communications (NCC).

As mutually supporting, fully integrated elements of the NCCIC, these branches provide the authorities, capabilities, and partnerships necessary to lead a whole-of-nation approach to addressing cybersecurity and communications issues at the operational level.

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

NO&I engages in planning, coordination, and integration capabilities to synchronize analysis, information sharing, and incident response efforts across the NCCIC's branches and activities.

US-CERT brings advanced network and digital media analysis expertise to bear on malicious activity targeting our nation's networks. US-CERT develops timely and actionable information for distribution to federal departments and agencies, state and local governments, private sector organizations, and international partners. In addition, US-CERT operates the National Cybersecurity Protection System (NCPS), which provides intrusion detection and prevention capabilities to covered federal departments and agencies.

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. Cybersecurity and infrastructure protection experts from ICS-CERT provide assistance to owners and operators of critical systems by responding to incidents and helping restore services, and by analyzing potentially broader cyber or physical impacts to critical infrastructure. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

NCC leads and coordinates the initiation, restoration, and reconstitution of National Security and Emergency Preparedness telecommunications services or facilities under all conditions. NCC leverages partnerships with government, industry and international partners to obtain situational awareness and determine priorities for protection and response.

The NCCIC also relies heavily on voluntary collaboration with its partners. The NCCIC works closely with those federal departments and agencies most responsible for securing the government's cyber and communications systems, and actively engages with private sector companies and institutions, state, local, tribal, and territorial governments, and international counterparts. Each group of stakeholders represents a community of practice, working together to protect the portions of critical information technology that they own, operate, manage, or interact with.

All media inquiries about the NCCIC and its missions, roles, and responsibilities should be directed to the Office of Cybersecurity and Communications (CS&C) External Affairs at cscexternalaffairs@hq.dhs.gov.

Related Resources

- National Protection and Programs Directorate
- Office of Cybersecurity and Communications
- Information Sharing
- Cyber Incident Response
- US-CERT
- ICS-CERT
- Careers in Cybersecurity
- NCCIC Org Chart 2014

Last Published Date: January 19, 2016