Homeland Security

NCCIC Services for Federal Agencies

The mission of the National Cybersecurity and Communications Integration Center (NCCIC) is to reduce the risk of systemic cybersecurity and communications challenges across public and private sector networks. NCCIC executes its mission by serving as the national hub for cyber and communications information, technical expertise, and operational integration, and by operating a 24/7 situational awareness, analysis, and incident response center.

NCCIC stakeholders include the Federal Government; state, local, tribal, and territorial (SLTT) governments; the private sector; and international partners. All services listed below are available at no cost.

Network Protection

EINSTEIN Program: NCCIC operates and manages the EINSTEIN program, which consists of systems to detect and prevent intrusions. EINSTEIN provides automated processes for collecting, correlating, analyzing, and sharing computer security information across the Federal Government to improve our Nation's cybersecurity posture.

Information Exchange

Automated Indicator Sharing (AIS): AIS is a machine-to-machine capability that receives, processes, and disseminates cyber threat indicators in real-time with the goal of reducing the number of cyber attacks.

NCCIC Portal: NCCIC manages a web-based platform that allows stakeholders to securely communicate, collaborate, and share cybersecurity information and TLP:GREEN and TLP:AMBER products within trusted communities of interest.

Website Resources: A variety of technical and non-technical TLP: WHITE products are available on the www.us-cert.gov and ics-cert.us-cert.gov websites. Users can also subscribe to receive email notifications as products become available.

Incident Response

NCCIC offers remote and on-site incident response capabilities, including expert intrusion analysis and mitigation guidance to customers who lack an in-house capability or require external assistance to manage a cyber incident. Technical services include network traffic analysis, host analysis, log analysis, and malware analysis.

The National Coordinating Center for Communications (NCC) coordinates 24/7 interagency and industry efforts to protect and restore communications during times of crisis.

Malware Analysis and Vulnerability Coordination

Advanced Malware Analysis Center: The Advanced Malware Analysis Center provides 24/7 dynamic analysis of malicious code. Samples may be submitted online using the "Report Malware" option on www.us-cert.gov.

Vulnerability Coordination: NCCIC works with trusted partners in the public and private sectors to coordinate timely and responsible disclosure of vulnerabilities. Risks are publicized only after practical and effective mitigations are available to users and administrators.

Cybersecurity Assessments

NCCIC offers a variety of assessments to help stakeholders proactively identify operational risks and measure their current security posture. These include Risk and Vulnerability Assessments, the Cyber Hygiene Program, Phishing Campaign Assessments, Red Team Assessments, and a downloadable Cyber Security Evaluation Tool (CSET).

Validated Architecture Design Reviews are conducted on Information Technology and Operation Technology. A team of experts evaluate the architecture, network traffic, and system logs—consulting with ICS subject matter experts as necessary.

Stakeholders receive recommendation and mitigation plans for all assessments.

Exercises and Training

Cyber Exercises: NCCIC supports continued improvement in national cyber preparedness and resilience through cyber exercise design, development, and conduct. Cyber Planning Workshops are offered to assist stakeholders with cyber incident response plan development.

Industrial Control Systems Training: Classroom and online training in industrial control systems security fundamentals is available for a range of learners. Regional courses and workshops are offered, including a five-day, hands-on training event in Idaho Falls, Idaho.

Public-Private Partnerships

Industrial Control Systems Joint Working Group (ICSJWG): ICSJWG supports information sharing and reduced risk to the nation's industrial control systems through enhanced collaboration between the Federal Government and private owners and operators of industrial control systems across all critical infrastructure sectors.

Communications Information Sharing and Analysis Center (ISAC): The National Coordinating Center for Communications (NCC) serves as the operational arm of the Communications Information Sharing and Analysis Center (Comm-ISAC) and facilitates the exchange of vulnerability, threat, and intrusion information.

Interagency Coordination

Joint Agency Cyber Knowledge Exchange (JACKE): NCCIC hosts a quarterly discussion of current threats and response strategies for cybersecurity professionals.

Security Operations Center (SOC) Coordination: NCCIC coordinates a weekly teleconference for SOC analysts to discuss tactical-level trends observed.

Federal Cybersecurity Interagency Group (FCIG): NCCIC organizes a monthly meeting for cybersecurity centers to collaborate on a variety of cybersecurity issues. Discussion topics include cybersecurity policy, operations, and technology use.

Contact Information

For more information on NCCIC services, contact **+1 (888) 282-0870** or ncciccustomerservice@hq.dhs.gov.
For more information on DHS cyber programs, visit **www.dhs.gov/cyber**.