Homeland Security

National Cybersecurity and Communications Integration Center

NCCIC/SECIR CYBER SERVICES

ORGANIZATION OVERVIEW

The National Cybersecurity and Communications Integration Center (NCCIC) shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

The Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) Division acts as the Department of Homeland Security (DHS) primary point of engagement and coordination for national security/emergency preparedness (NS/EP) communications and cybersecurity initiatives.

CRITICAL INFRASTRUCTURE CYBER COMMUNITY VOLUNTARY PROGRAM

The Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed") Voluntary Program seeks to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (the Framework), released in February 2014. The C³ Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. The C³ Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management. For more information or to contact us, please email: ccubedvp@hq.dhs.gov or www.dhs.gov/ccubedvp.

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)

The PCII program protects infrastructure information voluntarily shared with DHS to be used for homeland security purposes. The PCII program ensures that PCII in the government's hands is protected from disclosure.

ENHANCED CYBERSECURITY SERVICES (ECS)

ECS is a voluntary information sharing program that assists critical infrastructure owners and operators as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the Federal Government to gain access to a broad range of sensitive and classified cyber threat information. DHS shares this cyber threat information with qualified Commercial Service Providers to better protect critical infrastructure enterprises. More information is available at: http://dhs.gov/enhanced-cybersecurity-services.

CYBER INFORMATION SHARING AND COLLABORATION PROGRAM (CISCP)

A no-cost information sharing partnership between enterprises and DHS, CISCP creates shared situational awareness across critical infrastructure communities, enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents. For more information about CISCP, please email: ciscp_coordination@hq.dhs.gov.

CYBERSECURITY EVALUATION TOOL (CSET)

Industrial control systems security posture assessments, offered through CSET, a self-assessment tool. Features include a mapping to control systems standards based on the sector as well as a network architecture mapping tool. The tool can be downloaded for self-use or organizations can request a facilitated site visit, which could include basic security assessments, network architectural review and verification, network scanning using custom tools to identify malicious activity and indicators of compromise, and penetration testing. More information is available at: http://ics-cert.us-cert.gov/

Homeland Security

National Cybersecurity and Communications Integration Center

CYBER RESILIENCE REVIEW (CRR)

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise practices and procedures across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices. For additional information please see: http://us-cert.gov/ccubedvp/self-service-crr.

ALERTS, BULLETINS, TIPS, TRAINING

U.S. Computer Emergency Readiness Team (US-CERT) and Industrial Control System (ICS-CERT) develop alerts, bulletins, tips, technical documents including recommended practices as well as training available for all levels of stakeholders.

Access to alerts, bulletins, tips, and technical documents published by ICS-CERT and US-CERT. ICS-CERT also offers an extensive bibliography of relevant standards and references. Both sets of documents and references provide a better understanding of relevant control systems vulnerabilities and the measures critical infrastructure owners and operators can take to address them. More information on ICS-CERT and US-CERT alerts, bulletins, tips, technical documents, and training is available at: http://ics-cert.us-cert.gov and http://us-cert.gov.

In addition, US-CERT operates a secure portal and has a compartment (Cobalt) to serve as an information hub for enterprise systems security. Request access to Cobalt by sending an e-mail to COBALT@us-cert.gov with the subject line, "Request access to COBALT."

AUTOMATED INFORMATION SHARING

In its mission to help secure the U.S. Federal civilian networks and critical infrastructure, the NCCIC is leading a community effort to accelerate information sharing between network defense and incident response organizations and communities around the world. These efforts have taken the form of two technical specifications to enable secure, real-time, and actionable sharing activities:

TAXII™ - the Trusted Automated eXchange of Indicator Information, and STIX™ - the Structured Threat Information eXpression.

While DHS is leading the overall effort, the direction and design of TAXII and STIX is informed by a broad and diverse community which includes Computer Security Incident Response Teams (CSIRTs) from both the public and private sector, and many other participants from the field of network defense and cyber incident response. https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

NCCIC CONTACT INFORMATION

(888) 282-0870 / nccic@hq.dhs.gov

http://www.us-cert.gov/

http://malware.us-cert.gov/

http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

NCCIC CONTACT INFORMATION

http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience