Homeland Security

Cyber Information Sharing and Collaboration Program

The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) enables information exchange and the establishment of a community of trust between the Federal Government and critical infrastructure owners and operators. CISCP aims to foster collaboration with owners and operators by leveraging all areas of DHS' National Cybersecurity and Communications Integration Center (NCCIC). This collaboration can assist stakeholders with assessing cyber-related threats, vulnerabilities, and consequences so stakeholders can prevent, mitigate, or recover from cyber incidents.

PRODUCTS AND SERVICES

CISCP membership provides access to the full suite of NCCIC products, including services to support information exchange between Federal government partners and CISCP members.

NCCIC SERVICES

Monthly Analyst Calls
allow coordination on emerging threats and vulnerabilities

In-person Collaboration
occurs through the quarterly Technical and Training exchange meetings, and the Legal Discussion Working Group

Coordination with NCCIC Digital Analytics
for complimentary sample analysis

Cross-Sector Collaboration
for cyber analysis coordination

CISCP Analytical Products
delivered through an exclusive member portal

Automated Indicator Sharing
allows bi-directional sharing of cybersecurity information

Input on National Approaches
allows bi-directional sharing of cybersecurity information

Forum Post

Cyber Information Sharing and Collaboration Program

PRODUCTS AND SERVICES - *CONTINUED*

NCCIC PRODUCTS

Indicator Bulletins frequent, timely cyber threat information regarding indicators of compromise and vulnerabilities derived from government sources and CIKR owners and operators.

Analysis Reports in-depth analytical product that ties together related threat and intruder activity, describing the activity, how to detect it, defensive measures, and remediation advice.

Joint Analysis Report A report written between DHS and another Federal government entity to define or identify a cyber threat or vulnerability.

Malware Initial Findings Report A malware analysis report that provides initial indicators for computer network defense

Malware Analysis Report An in-depth analysis containing indicators as well as detailed descriptions of malware actions on an infected host and the code analysis with insight of specific Tactics, Techniques, and Procedures in the malware.

Joint Indicator Bulletins A product co-published between the NCCIC and another Federal entity containing domain names and IP addresses associated with on-going malicious activity.

THE CISCP MEMBERSHIP PROCESS

It's free to join and use the CISCP program. To become members, prospective critical infrastructure owners and operators sign Cooperative Research and Development Agreements (CRADAs). The CRADA enables DHS and the partner organization to exchange anonymized information. Once the CRADA is signed, DHS will coordinate a meeting to customize how DHS and the organization can exchange information.

For more information on joining CISCP, contact *CISCP_Coordination@hq.dhs.gov*.

PROTECTING THE INFORMATION EXCHANGE PROCESS

DHS uses the Protected Critical Infrastructure Information (PCII) Program to protect public and private sector infrastructure information voluntarily shared with the Federal Government for the purposes of homeland security. The PCII Program offers private-sector partners protection and confidence that the Federal Government will not expose sensitive or proprietary data shared through this program. Information shared through the program also adheres to the Traffic Light Protocol (TLP). For more information on the TLP, go to https://www.us-cert.gov/tlp.

CONTACT INFORMATION

www.dhs.gov/ciscp
CISCP_Coordination@hq.dhs.gov