Cyber Information Sharing and Collaboration Program (CISCP)

Information sharing is a key pillar of effective cybersecurity. By sharing information rapidly between the government and the private sector, network defenders are able to block cyber threats before damaging compromises occur. The Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) serves as the hub of information sharing activities for the Department to increase awareness of vulnerabilities, incidents, and mitigations. Within the NCCIC, the Cyber Information Sharing and Collaboration Program (CISCP) is DHS's flagship program for public-private information sharing and complements ongoing DHS information sharing efforts. In CISCP, DHS and participating companies share information about cyber threats, incidents, and vulnerabilities.

Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners. Further, CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses. CISCP is based upon a community of trust in which all participants seek mutual benefit from robust information sharing and collaboration. CISCP is free of charge and provides value to all members. Therefore, all companies with an interest in multi-directional cybersecurity information sharing and robust analytic collaboration between the government and the private sector should consider joining CISCP.

CISCP Products and Briefings

A key aspect of CISCP is bi-directional information sharing: CISCP partners submit indicators of observed cyber threats and information about cyber incidents and identified vulnerabilities to DHS, which DHS then shares with other CISCP partners in an anonymized, aggregated fashion. Upon receiving a submission, CISCP analysts redact any personal or proprietary information and analyze the submission in collaboration with both government and industry partners to produce accurate, relevant, timely and actionable analytical products. Currently, those products take the form of:

- **Indicator Bulletins (IB)**: Short, timely bulletins regarding new threats and vulnerabilities. These bulletins are sent several times a week in machine-readable formats. These formats enable faster parsing and analysis, resulting in faster action taken to thwart attacks and remediate vulnerabilities.
- **Analysis Report (AR)**: More in-depth analytic product that ties together related threat and intruder activity, describing the activity, how to detect it, defensive measures and remediation advice.
- **Priority Alert (PA)**: Focused on providing early warning of a single specific threat or vulnerability expected to have significant and far-reaching impact.
- **Recommended Practices (RP)**: Product that provides a method for collaboratively defining and documenting a series of "best practice" recommendations or strategies.

Information shared among CISCP partners is governed using the Traffic Light Protocol (TLP), which empowers the submitter to determine the handling and dissemination of their information. For more on TLP, visit http://us-cert.gov/tlp.

As part of CISCP, DHS facilitates collaboration events with government and industry partners, which foster a trusted environment for sharing cyber threat information. These exchanges are unclassified and focus on current threats or recent activity. In addition, the team hosts analyst-to-analyst technical threat exchanges and analyst training events that allow for classified and unclassified briefings.

Protecting Shared Information and Privacy

Data can be submitted to CISCP under Protected Critical Infrastructure Information (PCII) Program. Any PCII submissions are statutorily exempt from regulatory use or any disclosure under the Freedom of Information Act or state Sunshine Laws. However, PCII does not fulfill federal, state and local reporting requirements that may apply to specific organizations.

DHS embeds privacy protections and provides transparency in all of its cyber activities. DHS uses the Fair Information Practice Principles (FIPPs) to assess and mitigate impacts on an individual's privacy. For more information, visit the DHS Cybersecurity and Privacy web page.

Joining CISCP

To join CISCP, companies are required to sign a Cooperative Research and Development Agreement (CRADA). Along with governing participation in CISCP, a signed CRADA may permit access to the NCCIC watch floor and allows for company personnel to be eligible for security clearances to view classified threat information.

For more information about participating in CISCP, email ciscp_coordination@hq.dhs.gov.

Last Published Date: May 4, 2016