Homeland Security

CRITICAL INFRASTRUCTURE AND KEY RESOURCES CYBER INFORMATION SHARING AND COLLABORATION PROGRAM

ABOUT THE PROGRAM

The Critical Infrastructure Key Resources (CIKR) Cyber Information Sharing and Collaboration Program (CISCP) was established for information sharing and collaboration with our critical infrastructure partners. The CISCP shares cyber threat, incident, and vulnerability information in near-real time, and enhances collaboration in order to better understand the threat and improve network defense for the entire community. The key focus of this program is to establish a community of trust between the Federal Government and entities from across the different critical infrastructure sectors and then leverage these relationships for enhanced information sharing and collaboration.

JOINING THE PROGRAM AND PROTECTING THE INFORMATION SHARED

To join CISCP, partners such as Information Sharing and Analysis Centers (ISACs) and the stakeholder community – which consists of CIKR mature owners and operators – sign a Cooperative Research and Development Agreement (CRADA). The CRADA provides access to DHS's National Cybersecurity and Communications Integration Center (NCCIC) watch floor and clearances up to the TS/SCI level.

Within CISCP, government and industry partners contribute threat data adding to the volume of information currently available for analysis by the DHS CISCP analytical team.

Because the act of providing threat or attack data may harm competitive or other commercial interests of our industry partners, significant steps are taken to obscure the source of data provided. Data provided as Protected Critical Infrastructure Information (PCII) is also protected by statutorily exempting it from any release otherwise required by Freedom of Information or State Sunshine Laws, and by statutorily exempting it from regulatory use.

INFORMATION SHARING, PRODUCTS, AND COLLABORATION

CISCP participants submit indicators of observed cyber threat activity to DHS, which can be shared with other CISCP participants in an anonymized, aggregated fashion. Upon receiving a submission, CISCP analysts redact any personal or proprietary information and engage in analysis of the submission in collaboration with both government and industry to produce accurate, relevant, timely, actionable data and analytical products. Currently, those products take the form of:

- Indicator Bulletins: As an indicator of new threats and vulnerabilities these short, timely bulletins are based on reporting from government and CIKR, and are provided in machine-readable-language for ease of use.
- Analysis Bulletins: More in-depth analytic products that tie together related threats and intruder activity, describe the activity, discuss methods of detection and defensive measures, and provide general remediation information.
- Alert Bulletins: Products providing an early warning of a single specific threat or vulnerability expected to have significant CIKR impact. The Alert Bulletins include mitigation recommendations and are provided in plain text for ease of use by the data consumer.

Homeland Security

- Recommended Practices: Products providing best practice recommendations and strategies for threat detection, prevention, and mitigation.

Information shared among CISCP partners and stakeholders is governed using the Traffic Light Protocol (TLP), empowering the submitters to determine the handling and dissemination of their information. For more on the TLP, please visit **https://us-cert.gov/tlp.**

In an effort to build a trusted environment for sharing information of this nature, the CISCP Operations Team facilitates key collaboration events including both government and program participants. The CISCP Operations Team hosts a technical teleconference between CISCP analysts at DHS and industry analysts. These exchanges are strictly unclassified and tend to focus on current threats or recent activity.

In addition, the team hosts analyst-to-analyst technical threat exchanges and analyst training events which allow for classified and unclassified briefings. They include government and industry partners sharing details of cyber threat activity, and mitigation recommendations and strategies.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. DHS actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets.

For more information, please visit www.dhs.gov/cyber.

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