

STOP.THINK.CONNECT.™

Department of Homeland Security Industry Offerings, Products, and Services

The Department of Homeland Security (DHS) partners with the public and private sectors to improve the Nation's cyber infrastructure.

PARTNERSHIP OPPORTUNITIES

The **Critical Infrastructure Partnership Advisory Council (CIPAC)** is a partnership between government and critical infrastructure owners and operators, which provides a forum to engage in a broad spectrum of critical infrastructure protection activities, like the **Cross-Sector Cyber Security Working Group**. To learn more, visit: <http://www.dhs.gov/cipac>.

The **Industrial Control Systems Joint Working Group** facilitates information sharing between the Federal Government and private sector owners and operators in all critical infrastructure sectors to reduce the risk of cyber threats to the Nation's Industrial Control Systems. For more information, visit http://www.us-cert.gov/control_systems/icsjwg/ or contact icsjwg@dhs.gov.

INCIDENT RESPONSE CAPABILITIES

The **United States Computer Emergency Readiness Team (US-CERT)** collaborates with Federal, State, Local, tribal, and territorial governments, the private sector, the research community, and international entities to monitor cyber trends. US-CERT provides access to actionable situational awareness reports; detection information about emerging cyber threats and vulnerabilities; and cybersecurity warning and alert notifications through the **National Cyber Alert System**. Visit <http://www.us-cert.gov/cas/signup.html> to subscribe to these free resources.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates industrial control systems-related security incidents and information sharing through **Fly-Away (Incident Response) Teams** with its public and private sector constituents, as well as international and private sector CERTs. ICS-CERT also operates a **Malware Lab** to analyze vulnerabilities and malware threats to ICS equipment. For additional information visit http://www.us-cert.gov/control_systems/ics-cert/. To report suspicious cyber activity affecting ICS, call the ICS-CERT Watch Floor at (877) 776-7585 or email ics-cert@dhs.gov.

OUTREACH & AWARENESS

DHS collaborates with its partners, including the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center, to support public outreach and awareness activities, including **National Cyber Security Awareness Month** and the **Stop.Think.Connect.** Campaign. To learn more or to book a speaker for an upcoming event, visit <http://www.dhs.gov/cyber> or <http://www.dhs.gov/stopthinkconnect>.



Homeland
Security



STOP | THINK | CONNECT™

CYBER ASSESSMENTS, EVALUATIONS, AND REVIEWS

The **Cyber Security Evaluation Program (CSEP)** performs **Cyber Resilience Reviews (CRRs)**, which measure adoption of maturity aspects of cybersecurity risk management using a common, capability-based framework. A CRR serves as a repeatable cyber review of an organization's ability to manage cybersecurity and ensure core process-based capabilities exist. For more information, contact the program at CSE@dhs.gov.

The **Cyber Security Evaluation Tool (CSET)** provides a systematic and repeatable approach to assess the cybersecurity posture of ICS networks. CSET is a stand-alone software tool that enables users to assess their network and ICS security practices against industry and government standards and it provides prioritized recommendations. To request a CSET CD, email cset@dhs.gov. For all other questions, email cssp@dhs.gov or visit http://www.us-cert.gov/control_systems/.

The **Cybersecurity Assessment and Risk Management Approach (CARMA)** is used to assist critical infrastructure sectors; State, local, tribal, and territorial governments; and other public and private sector partners in their efforts to assess, prioritize, and manage cyber infrastructure risk by providing a picture of sector-wide risks for different categories of cyber critical infrastructure. For more information, email NCSD_CIPCS@dhs.gov.

EDUCATION AND WORKFORCE DEVELOPMENT INITIATIVES

DHS and the National Security Agency (NSA) co-sponsor the **National Centers of Academic Excellence** in Information Assurance Education (CAE/IA), CAE-Research (CAE-R), and the two-year (CAE2Y) programs. These programs promote higher education in cybersecurity and produce growing numbers of IA workers. For more information, visit http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml.

DHS and the National Science Foundation offer the **Scholarship for Service Program (SFS)** to outstanding undergraduate, graduate, and doctoral students in exchange for government service at a Federal agency. SFS is building a strong pipeline of skilled employees to fill critical IA positions. For more information, see <https://www.sfs.opm.gov>.

EXERCISES AND TRAINING

The **Cyber Storm Exercise Series** focuses on simulated cyber-specific threat scenarios intended to highlight critical infrastructure interdependence and further integrate Federal, State, international, and private sector response and recovery efforts. The series helps participants assess their response and coordination capabilities specific to a cyber incident. Contact CEP@dhs.gov for more information.

SOFTWARE ASSURANCE ASSISTANCE

The **Software Assurance Forum** brings public and private stakeholders together to discuss ways to advance software assurance objectives. Through collaborative events, stakeholders raise expectations for product assurance with requisite levels of integrity and security, and promote security methodologies and tools as a normal part of business.

“**Build Security In**” (BSI) is a collaborative effort to provide tools, guidelines, and other resources, which software developers, architects, and security practitioners can use to build security into software in every phase of development. For information, visit: <https://buildsecurityin.us-cert.gov/swa> or email software.assurance@dhs.gov.

