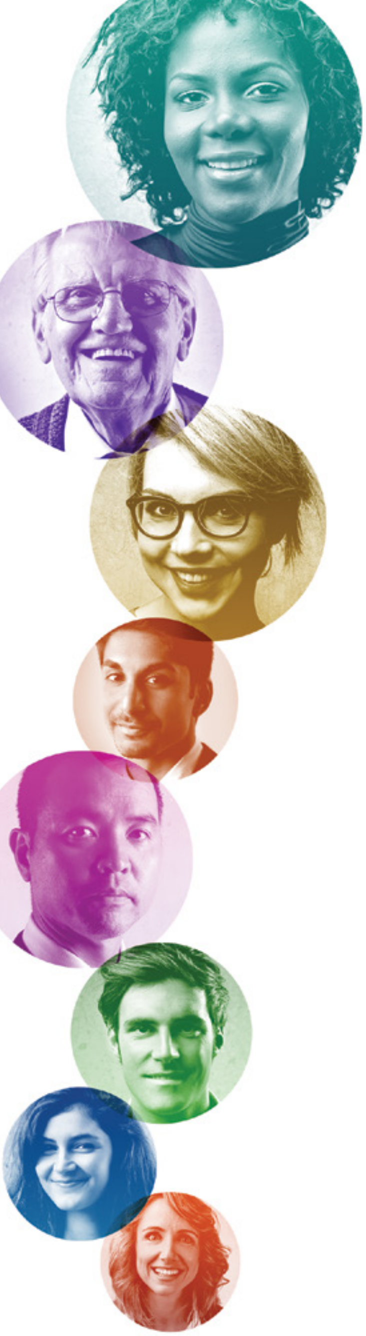


DEPARTMENT OF HOMELAND SECURITY

FEDERAL GOVERNMENT OFFERINGS, PRODUCTS, AND SERVICES

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

CRITICAL INFRASTRUCTURE CYBER COMMUNITY VOLUNTARY PROGRAM (C3VP)

DHS launched the **Critical Infrastructure Cyber Community Voluntary Program** 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 C^3 Voluntary Program was created to help improve the resiliency of critical infrastructure's cybersecurity systems by supporting and promoting the use of the Framework. For more information, visit www.us-cert.gov/ccubedvp.

PARTNERSHIP OPPORTUNITIES

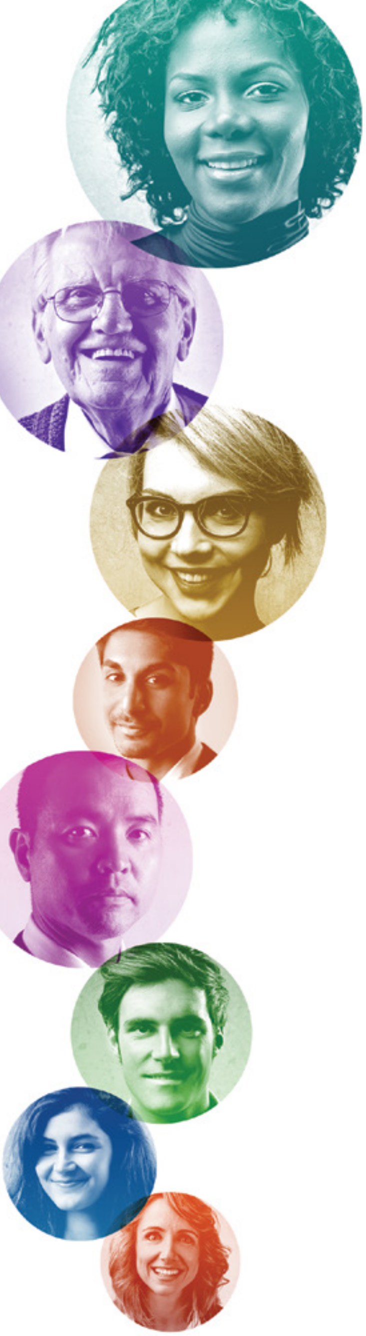
The **Critical Infrastructure Partnership Advisory Council (CIPAC)** is a partnership between government and critical infrastructure owners and operators, which provides a forum to engage in a broad spectrum of critical infrastructure protection activities, like the Cross-Sector Cyber Security Working Group. To learn more, visit: 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 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 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 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 request a speaker for an upcoming event, visit www.dhs.gov/cyber or www.dhs.gov/stopthinkconnect.

CYBER ASSESSMENTS, EVAULATIONS, 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, visit www.us-cert.gov/ccubedvp/self-service-crr.

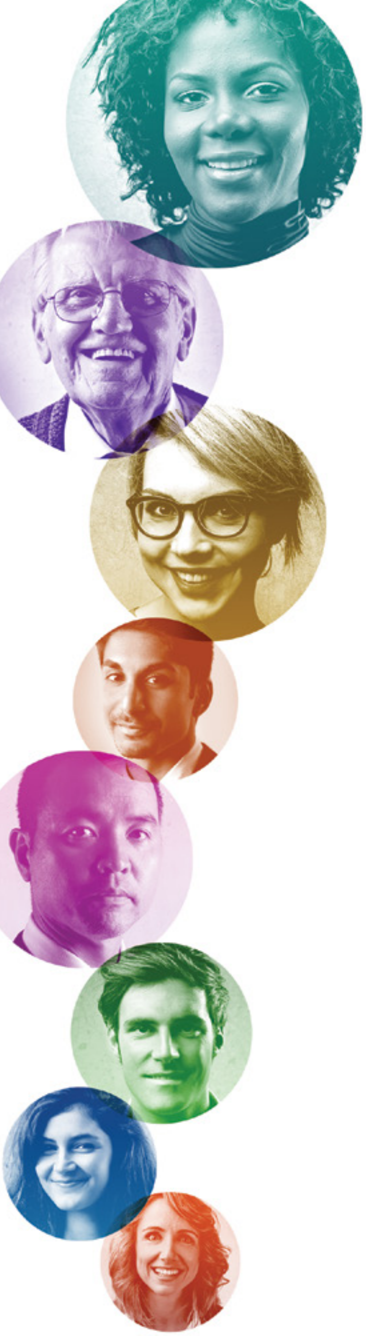
The **Cyber Security Evaluation Tool (CSET)** provides a systematic and repeatable approach to assess the cybersecurity posture of ICS networks. CSET is a stand-alone software tool that enables users to assess their network and ICS security practices against industry and government standards and it provides prioritized recommendations. For more information, visit www.ics-cert.us-cert.gov/assessments.

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 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 positions. For more information, see www.sfs.opm.gov.

The DHS Office of Cybersecurity Education & Awareness offers multiple training and education resources, including an extensive Training Catalog where cybersecurity professionals, and those entering cybersecurity careers, can quickly identify the courses they need to advance within their specialty area or to transfer skills. DHS also contributed to the development of the **National Cybersecurity Workforce Framework**, which is the foundation for increasing the size and capability of the US cybersecurity workforce. Tools and resources are available for organizations to learn how to use the Workforce Framework and assess their own cybersecurity workforce needs. Government personnel can also receive free cybersecurity training through the on-demand Federal Virtual Training Environment (FedVTE) and live Federal Cybersecurity Training Events (FedCTE). For more information, visit www.niccs.us-cert.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 cyberstorm@hq.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: www.buildsecurityin.us-cert.gov/swa or email software.assurance@dhs.gov.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit http://www.dhs.gov/stopthinkconnect.

Homeland Security

www.dhs.gov/stopthinkconnect

STOP | THINK | CONNECT™