Control Systems Security Program

ONSITE CONSULTATION AND SELF-EVALUATION

The Department of Homeland Security's (DHS) Control Systems Security Program (CSSP) assists owners of networks and industrial control systems (ICS) in assessing and strengthening their organization's cybersecurity posture. Through a tiered system including the Cyber Security Evaluation Tool (CSET®) and onsite consultation options, CSSP helps ICS asset owners take the preventative measures necessary to prepare for and protect from cyber attacks.

CUSTOMIZABLE SUPPORT

With the increasing threat of cyber attacks, CSSP is seeking to expand awareness of defense-in-depth strategies for cybersecurity. A tiered approach allows asset owners and operators to select the level of CSSP support needed to meet their operational needs.

Onsite consultations are offered at no cost to asset owners and provide an opportunity to examine organizations' cybersecurity posture with the assistance of DHS's cybersecurity subject matter experts.

CSSP TIERED APPROACH

- CSET Self-Assessment
- Tier 1: CSET System and Process Evaluation
- Tier 2: Network Architecture Review

CSET SELF-ASSESSMENT

The CSET is a self-contained software tool which runs on a desktop or laptop. Asset owners can leverage the CSET application to evaluate the cybersecurity posture of an automated, industrial control or business system. CSET uses a hybrid risk and standards-based approach, and provides relevant recommendations for improving the security of an organization. CSSP developed the CSET application, and offers it to all through the Control Systems Security Program website.

TIER 1 – CSET SYSTEM AND PROCESS EVALUATION

Tier 1 offers an onsite consultation provided by CSSP cybersecurity staff at asset owners' facilities. The asset owners leverage the CSET application, while receiving technical guidance from the CSSP consultation team.

The Tier 1 consultation focuses on identifying the primary vulnerabilities and improvements for asset owners using industry recognized cybersecurity standards as the basis for performance. Tier 1 consultations are typically conducted in one day with one or two of CSSP's experienced subject matter experts, along with the asset owners and key staff. The consultation provides a quick and effective analysis of the control system and its core functions, infrastructure, and policies and procedures. A Tier 1 consultation is generally sufficient for assets that support most critical facilities and infrastructures.

TIER 2 – NETWORK ARCHITECTURE REVIEW

Tier 2 consultation offers a network architecture review and analysis, which can be completed independent of, or in conjunction with, a CSET self-assessment or system and process evaluation. The network architecture review includes a comprehensive evaluation and discovery process, focusing on defense strategies associated with asset owners' specific control systems network. This process may include an in-depth review and evaluation of control systems network design, configuration and application.

Homeland Security

The Tier 2 assessment, like Tier 1, is conducted onsite by the asset owners with the support of CSSP cybersecurity professionals. However, the Tier 2 consultation provides a more robust evaluation of system interdependencies, vulnerabilities, and mitigation options. This consultation typically requires additional rigor and technical staff and often takes two to three days to complete. As part of the review, experts examine information related to key control systems external connections and conduct an extensive review of control system design documents, drawings, and architectures. This assessment is likely to be useful for most high-security control systems, such as chemical, power and nuclear plants, telecommunications facilities, government facilities, schools, hospitals, and other high-value infrastructure assets.

CROSS-FUNCTIONAL COOPERATION

In order to garner the most accurate and useful results from the CSET application and CSSP onsite consultations, coordination with subject matter experts from across the ICS organization is vital. This cross-functional team often consists of representatives from the operational, maintenance, information technology, business, and security divisions. The organization's team can prepare to participate in a CSET self-assessment or CSSP onsite consultation by reviewing their policies and procedures, network topology diagrams, inventory lists of critical assets and components, risk assessments, and organizational roles and responsibilities.

CONSULTATION PREPARATION

When planning and organizing for an onsite consultation, the following is recommended:

- Identify the cross-functional assessment team members from your organization and schedule a date.
- Ensure cross-functional assessment team members have reviewed relevant information and are adequately prepared to participate in the consultation session.
- Select a meeting location to accommodate the consultation team during the question and answer portion of the assessment.

BENEFITS OF CSSP SUPPORT

By leveraging the CSET application and CSSP onsite consultation opportunities, asset owners can increase the cybersecurity posture of their organization. Some key benefits include:

- Highlighting vulnerabilities in the organization's systems and providing recommendations on ways to address them;
- Identifying areas of strength and recommended practices being followed in the organization;
- Providing a method to systematically compare and monitor cyber systems improvement;
- Informing an organization's risk management and decision-making process; and
- Raising awareness and facilitating discussion on cybersecurity within the organization.

REQUEST CSSP SUPPORT

To learn more about CSET or to download a copy, visit www.us-cert.gov/control_systems.

To request a Tier 1 or Tier 2 onsite consultation, send an email to cset@dhs.gov.

For general program questions or comments, contact cssp@dhs.gov.

ABOUT CSSP

DHS created the National Cyber Security Division's CSSP to reduce industrial control system risks within and across all critical infrastructure and key resource sectors.

For more information, visit www.us-cert.gov/control_systems.