



The Cyber Security Evaluation Tool (CSET) provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system networks. It also includes both high-level and detailed questions applicable to all industrial control systems (ICS).

CSET was developed under the direction of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) by cybersecurity experts with assistance from the National Institute of Standards and Technology. CSET is a desktop software tool that guides users through a step-by-step process to assess their control system network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of an organization's ICS or enterprise network. CSET derives the recommendations from a database of cybersecurity standards, guidelines, and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.

CSET Assessment Process

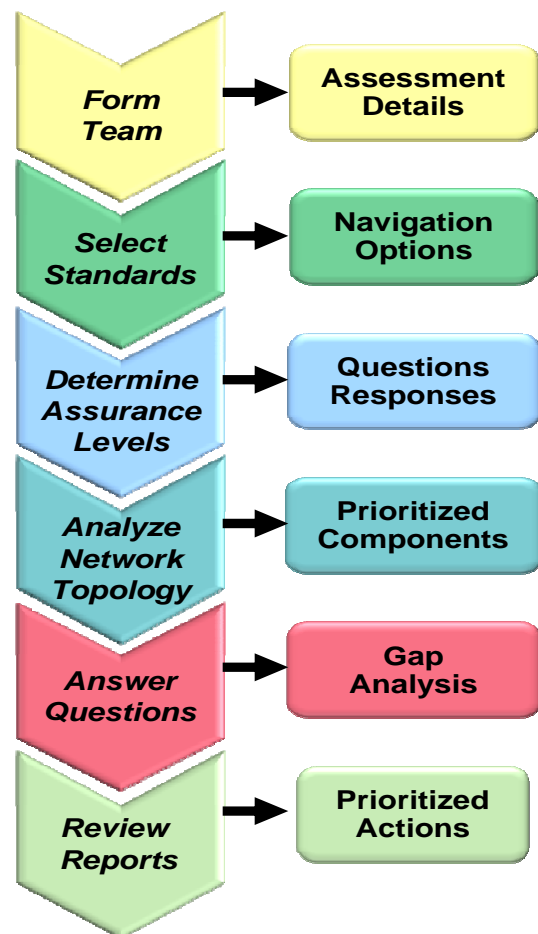
The assessment process is accomplished by following the six steps outlined below and shown in Figure 1:

Form Team: A team is formed by selecting cross-functional resources consisting of personnel familiar with the various operational areas in an organization. For example, in the ICS environment, teams typically include representatives that are familiar with the ICS details such as senior management, operations, information technology, ICS engineers, and security (physical and cyber). Organizations may add additional team members depending on the skills and/or expertise required to complete the assessment process.

Select Standards: CSET provides a list of security standards under the "Navigation" tab within the tool. Based on the user's selections, CSET generates questionnaires associated with these standards for use in the assessment process.

Determine Assurance Level: The Security Assurance Level (SAL) is based on the user's answers to a series of questions related to the potential worst-case consequences of a successful cyber attack. CSET will calculate a recommended SAL for the facility or subsystem being assessed and then provide the level of security rigor needed to protect against a worst-case event. For National Institute of Standards and Technology (NIST)-based standards and guidance, CSET also supports the Federal Information Processing Standards (FIPS) 199 guidelines for determining the security categorization of a system.

Figure 1: CSET Process Flow





Analyze Network Topology: CSET contains a graphical user interface which allows users to build the control system network topology (including criticality levels) into the CSET software. By creating a network architecture diagram which is based on components deemed critical to the organization, users are able to define the organizations cybersecurity boundary and posture. An icon palette is provided for the various system and network components, allowing users to build a network architecture diagram by dragging and dropping components onto the screen.

Answer Questions: CSET generates questions based on the specified network topology, the SAL, and the security standards that were selected. The assessment team then selects the best answer to each question based on the system's network configuration and implemented security practices. CSET compares the answers provided by the assessment team with the recommended security standards and generates a list of security gaps and/or recognized good practices.

Review Reports: CSET generates interactive or printed reports. The reports provide a summary of security level gaps or areas that did not meet the recommendations of the selected standards. The assessment team may then use this information to plan and prioritize mitigation strategies.

Assessment Logistics and Onsite Visits

CSSP may provide "over-the-shoulder" training and guidance to asset owners in using CSET during onsite assessments. To assist an organization in planning and organizing for an assessment using the CSET, the following actions and items are recommended:

- Identify the assessment team members and schedule a date.
- Become familiar with information about the organization's system and network by reviewing policies and procedures, network topology diagrams, inventory lists of critical assets and components, risk assessments, IT and ICS network policies/practices, and organizational roles and responsibilities.

- Select a meeting location to accommodate the assessment team during the question and answer portion of the assessment.
- Work with CSSP for onsite or subject matter support.

Typical DHS Control Systems Security Program Onsite Assessment

An example agenda for an onsite assessment from CSSP would include the following activities:

1. **ICS Awareness Briefing** – 1 hour
 - Cyber security awareness briefing
 - CSET training and demonstration
2. **IT and Enterprise Network Evaluation** – 4 hours
 - Policies and practices evaluation
 - IT and control system interfaces
 - Network component evaluation
3. **ICS Evaluation** – 4 to 6 hours
 - Security Assurance Level determination
 - Network topology evaluation
 - Component questionnaire
4. **Review/Wrap-up** – 2 hours
 - Generate reports and review security gaps
 - Close-out briefing and recommendations

Obtaining Additional Information

To learn more about the CSET, contact cset@dhs.gov. For general program questions or comments, contact cssp@dhs.gov or visit http://www.us-cert.gov/control_systems/.

About DHS and NCSD

The Department of Homeland Security (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. The National Cybersecurity Division (NCSD) leads the DHS efforts to secure cyberspace and our Nation's cyber assets and networks.