Homeland Security

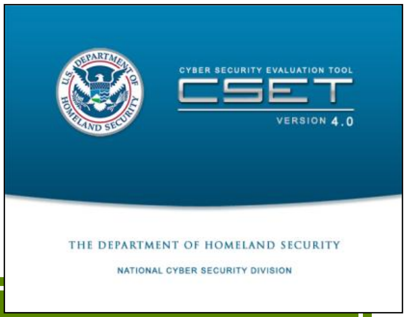
Cyber Security Evaluation Tool (CSET)

Performing a Self-Assessment

The Cyber Security Evaluation Tool (CSET) provides users with a systematic and repeatable approach for assessing the cybersecurity posture of their industrial control system networks. This tool 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).

What is it?

The CSET is a stand-alone desktop software tool that enables users to assess their network and ICS security practices against recognized industry and government standards, guidelines, and practices. The completed CSET assessment provides a prioritized list of recommendations for increasing the cybersecurity posture of an organization’s ICS or enterprise network and identifies what is needed to achieve the desired level of security within the specific standard(s) selected.


CYBER SECURITY EVALUATION TOOL
CSET
VERSION 4.0
THE DEPARTMENT OF HOMELAND SECURITY
NATIONAL CYBER SECURITY DIVISION

Downloadable via the Internet at:
http://us-cert.gov/control_systems/csetdownload.html

The Assessment Process

Four basic steps are available to complete an assessment using CSET. The process is shown in the CSET Process Flow figure.

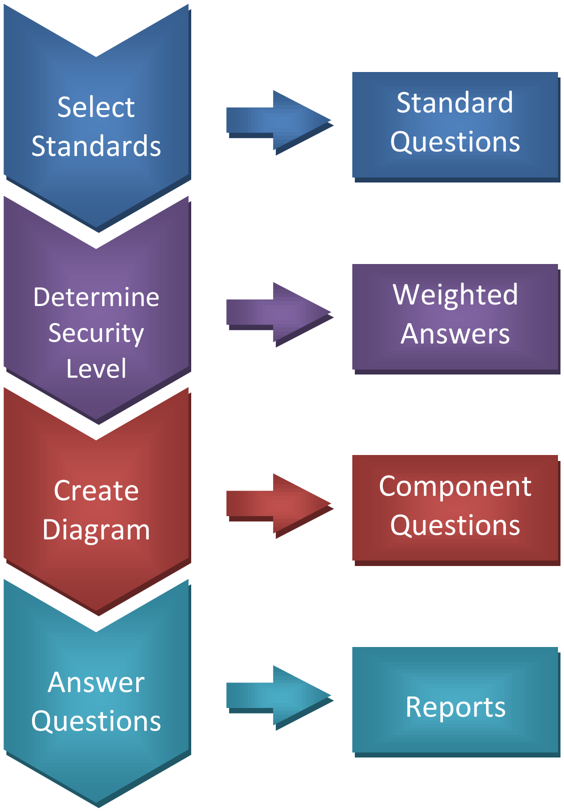
STEP 1-Select Standards: Users are given the option to select one, several, or all the following industry and government-recognized cybersecurity standards.

Security Standards

- **DHS Catalog of Control Systems Security: Recommendations for Standards Developers, Revisions 6 and 7**
- **NIST SP800-82**
- **NIST SP800-53, revision 3**
- **NRC Regulatory Guide 5.71**
- **CFATS Risk Based Performance Standard (RBPS) 8**
- **NERC CIP-002-009 revisions 2 and 3**
- **ISO/IEC 15408 revision 3.1**
- **DoDI 8500.2**
- **Consensus Audit Guidelines 2.3.**

After the user selects the applicable standard(s), CSET generates questions that are specific for those requirements.

CSET Process Flow



http://www.us-cert.gov/control_systems/satool.html

Cyber Security Evaluation Tool (CSET)

Performing a Self-Assessment

STEP 2-Determine Assurance Level: The basis for a Security Assurance Level (SAL) is the user's answers to a series of questions relating to the potential worst-case consequences of a successful cyber attack. CSET calculates a SAL recommendation for the ICS organization, facility, system, or subsystem assessment. CSET then provides the level of cybersecurity rigor necessary 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. Upon SAL completion, CSET determines and reports the security gaps using comparative analysis between the answers to standards questions and the SAL.

STEP 3-Create Diagram: CSET contains a graphical user interface that allows users to build the control system network topology (including criticality levels) into the CSET software. By creating a network architecture diagram using components deemed critical to the organization, users are able to define the organizations cybersecurity boundary and posture. CSET provides icon palettes for the various system and network components, allowing users to build a network architecture diagram by dragging and dropping components onto the screen. Specific questions direct the identification of each network component.

STEP 4-Answer Questions: CSET generates questions using the specified network topology and the selected security standards as its basis. The assessment team then selects the best answer to each question using the system's network configuration and implemented security practices. CSET compares the assessment team answers with the recommended security standards and generates a list of recognized good practices and/or security gaps.

CSET generates both interactive (on-screen) and 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.

Onsite Assessment

CSSP provides "over-the-shoulder" training and guidance to assist asset owners in using CSET for the first time.

In order to assist an organization in planning and organizing for an assessment using the CSET, the key staff should become familiar with information about the organization's system(s) and network(s) by reviewing polices 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.

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
2. IT and Enterprise Network Evaluation
3. ICS Evaluation
4. Review/Closeout Briefing.

Obtaining Additional Information

To learn more about the CSET or to request a software copy via CD, 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 Cyber Security Division (NCSD) leads the DHS efforts to secure cyberspace and our nation's cyber assets and networks.