



Protecting Cyber Assets

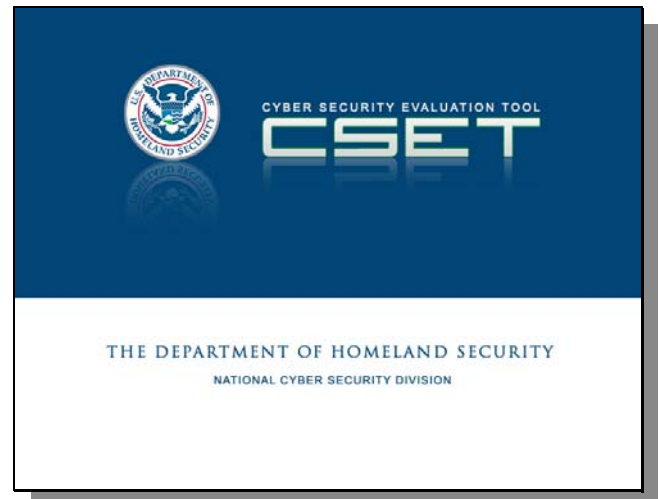
The Department of Homeland Security (DHS) is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. The National Cyber Security Division (NCSD) coordinates the Department's efforts to secure cyberspace and our nation's cyber assets and networks.

Critical infrastructures are dependent on information technology systems and computer networks for essential operations. Particular emphasis is placed on the reliability and resiliency of the systems that comprise and interconnect these infrastructures. NCSD collaborates with partners from across public, private, and international communities to advance this goal by developing and implementing coordinated security measures to protect against cyber threats.

The Cyber Security Evaluation Tool (CSET) is a DHS product that assists organizations in protecting these key national cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks.

Key Benefits

- CSET contributes to an organization's risk management and decision-making process
- Raises awareness and facilitates discussion on cybersecurity within the organization
- Highlights vulnerabilities in the organization's systems and provides recommendations on ways to address the vulnerability
- Identifies areas of strength and best practices being followed in the organization
- Provides a method to systematically compare and monitor improvement in the cyber systems
- Provides a common industry-wide tool for assessing cyber systems



Tool Features

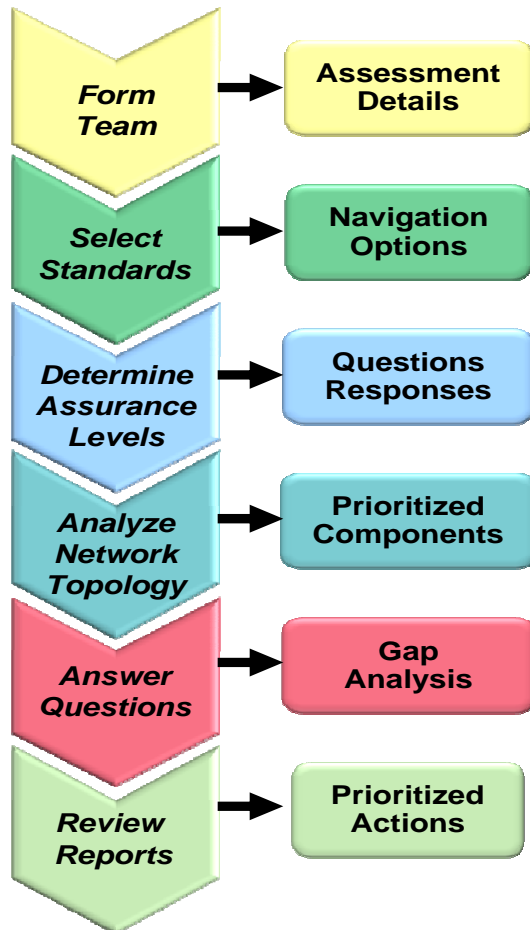
CSET is a desktop software tool that guides users through a step-by-step process to assess their cyber systems and network security practices against recognized industry standards.

The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's business and industrial control systems (ICS). CSET derives the recommendations from a database of cybersecurity standards and practices. Each recommendation is linked to a set of actions that can be applied to enhance cybersecurity controls.

CSET has been designed for easy install and use on a stand-alone laptop or workstation. It incorporates a variety of available standards from organizations such as National Institute of Standards and Technology (NIST), North American Electric Reliability Corporation (NERC), International Organization for Standardization (ISO), U.S. Department of Defense (DOD) and others. When the tool user selects one or more of the standards, CSET will open a set of associated questions. The answers to these questions are compared against a selected security assurance level and a detailed report is generated to show areas for potential improvement.



Figure 1: CSET Process Flow



Self-Assessment Process

The self-assessment process is accomplished by following the six steps outlined below and shown in Figure 1. Assistance in using CSET to perform a self-assessment may also be requested from DHS.

Form Team: A team is formed by selecting cross-functional resources consisting of personnel familiar with the various operational areas in the organization.

Select Standards: CSET provides a list of security standards under the “Navigation” tab within the tool. It also includes the option to perform an enterprise evaluation that is a higher level assessment of any cyber system. Different question sets are displayed depending on the navigation selection.

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 calculates a recommended SAL for the facility or subsystem being assessed and then provides the level of security rigor needed to protect against a worst-case event. For NIST-based standards and guidance, CSET also supports the Federal Information Processing Standards (FIPS) 199 process for determining the security categorization of a system.

Analyze Network Topology: CSET contains a graphical user interface, which allows users to build the system network 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.

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 configuration and implemented security practices.

Review Reports: CSET generates interactive or printed reports. It 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. The interactive report also provides direct access to documentation to assist in understanding and addressing the weakness. The assessment team may then use this information to plan and prioritize mitigation strategies.

Obtaining Addition Information

To learn more about the CSET, please contact: CSET@dhs.gov

or visit: http://www.us-cert.gov/control_systems/