Control Systems Security Program

CYBER SECURITY EVALUATION TOOL

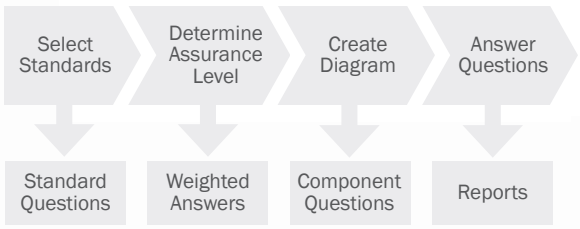
PERFORMING A SELF-ASSESSMENT

The Cyber Security Evaluation Tool (CSET®) is a self-contained software tool which runs on a desktop or laptop computer. It evaluates the cybersecurity of an automated, industrial control or business system using a hybrid risk and standards-based approach, and provides relevant recommendations for improvement. The Department of Homeland Security's (DHS) Control Systems Security Program (CSSP) developed the CSET application, and offers it to all through the United States Computer Emergency Readiness Team's (US-CERT) website.

HOW IT WORKS

CSET helps asset owners to assess their information and operational systems cybersecurity practices by asking a series of detailed questions about system components and architecture, as well as operational policies and procedures. These questions are derived from accepted industry cybersecurity standards.

Once the self-assessment questionnaire is complete, CSET provides a prioritized list of recommendations for increasing cybersecurity posture, including solutions, common practices, compensating actions, and component enhancements or additions. The tool also identifies what is needed to achieve a desired level of cybersecurity within a system's specific configurations.



THE ASSESSMENT PROCESS

All industry sectors can benefit from CSET's simple process for evaluating and improving their automated and industrial control systems (ICS) using these four basic steps.

1. SELECT STANDARDS

To get started, users are invited to select one or more of the following government and industry recognized cybersecurity standards. CSET then generates questions that are specific to those requirements.

- CFATS Risk Based Performance Standard (RBPS) 8: Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
- DHS Catalog of Control Systems Security: Recommendations for Standards Developers, Revisions 6 and 7
- DoD Instruction 8500.2 Information Assurance Implementation, February 2, 2003
- ISO/IEC 15408 revision 3.1: Common Criteria for Information Technology Security Evaluation, Revision 3.1
- NERC Reliability Standards CIP-002-009 Revisions 2 and 3
- NIST Special Publication 800-82 Guide to Industrial Control Systems Security, June 2011
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems Rev 3 and with Appendix I, ICS Controls
- NRC Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities, January 2010

Homeland Security

2. DETERMINE ASSURANCE LEVEL

The security assurance level (SAL) is determined by responses to questions relating to the potential consequences of a successful cyber attack on an ICS organization, facility, system, or subsystem. CSET then calculates a SAL and provides a recommended level of cybersecurity rigor necessary to protect against a worst-case event. Using the SAL to determine the required level of security, CSET runs a comparative analysis between the requirements identified in the standards selected and the answers provided by the user.

For assessments using the National Institute of Standards and Technology (NIST) standards and guidance, CSET also supports the Federal Information Processing Standards (FIPS) 199 guidelines for determining the security categorization of a system.

3. CREATE DIAGRAM

CSET contains a graphical user interface that allows one to diagram the control system network topology and identify the "criticality" of the network components. By creating a network architecture diagram, users are able to define the organization's cybersecurity zones, critical components, and communications conduits. An icon palette featuring various system and network components allows users to build diagrams by simply dragging and dropping them into place. Specific questions further facilitate the detailed identification of each component.

4. ANSWER QUESTIONS

CSET then generates questions using the network topology and selected security standards as its basis. The assessment team selects the best answer to each question using the organization's actual network configuration and implemented security policies and procedures. The tool compares the completed answers with the recommended requirements from the standards and generates a list of recognized good practices and security gaps. CSET also 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.

CSET AT-A-GLANCE

Over the past few years, CSSP has assisted with numerous onsite self-assessments across the country and in all critical infrastructure sectors. In 2011, ICS owners and operators downloaded more than 1,600 copies of CSET and CSSP helped perform 81 self-assessments in 26 states. Sectors with the highest number of self-assessments include: water and water treatment, energy, transportation, commercial and government facilities, and public health/healthcare.

The CSSP team observed that the most common vulnerabilities identified through CSET self-assessments were a lack of adequate control system inventories and formal documentation; no audit capabilities and accountability for event monitoring; and missing permissions, privileges, and access control restrictions. Other categories of vulnerabilities included improper authentication and credentials management practices, flaws in network architecture designs, configuration (implementation) settings within network components, and traceability on cybersecurity configuration and maintenance.

To assist an organization in planning for a CSET self-assessment, key staff should become familiar with information about the organization's ICS components, understanding the complete list of assets, including all operational hardware assets and components, as well as software for all user interfaces. Staff should also understand data exchanges and operational data flow. To adequately prepare for a CSET self-assessment, staff should review policies and procedures, network topology diagrams, inventory lists of critical assets and components, risk assessments, IT and ICS network policies and practices, and organizational roles and responsibilities.

GETTING STARTED

Get started by downloading CSET at www.us-cert.gov/control_systems/csetdownload.html.

To learn more about CSET or to request a CD copy of the software, contact cset@dhs.gov.

For general program questions or comments, contact cssp@dhs.gov or visit www.us-cert.gov/control_systems.

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.