Homeland Security

Control Systems Security Program
Performing a Self- Assessment Using CS^{2}SAT

The Control Systems Cyber Security Self-Assessment Tool (CS^{2}SAT) provides users with a systematic and repeatable approach for assessing the cyber security posture of their industrial control system networks. The CS^{2}SAT was developed under the direction of the Department of Homeland Security (DHS) Control Systems Security Program (CSSP) by cyber security experts and with assistance from the National Institute of Standards and Technology. The CS^{2}SAT is a desktop software tool which guides users through a step-by-step process to assess their control system network security practices against recognized industry standards. The output from the CS^{2}SAT is a prioritized list of recommendations for improving the cyber security posture of the organization's industrial control systems (ICS) environment. The CS^{2}SAT derives the recommendations from a database of cyber security standards and practices, which have been adapted specifically for application to the ICS architecture and components. Each recommendation is linked to a set of actions that can be applied to enhance cyber security controls.

Self-Assessment Process

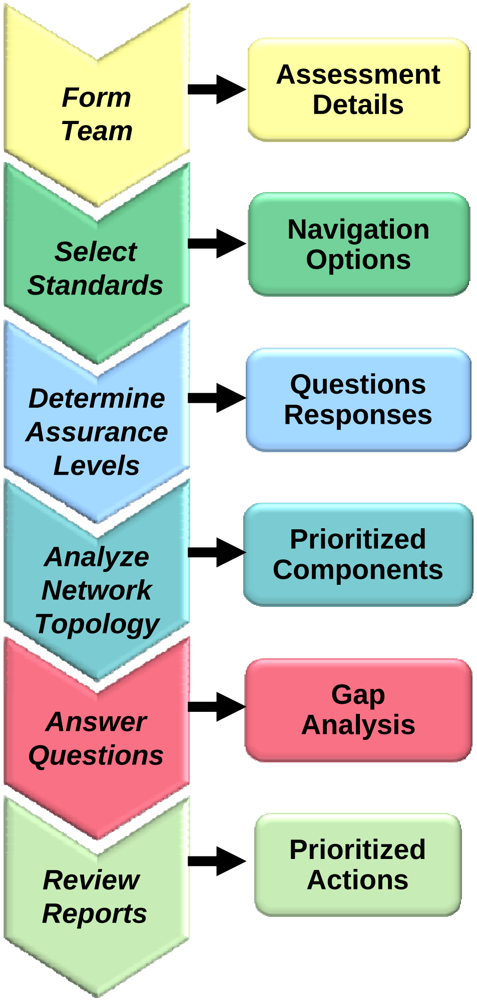
Assistance in using the CS^{2}SAT to perform a self-assessment may be requested from the CSSP. The Self-Assessment process is accomplished by following the six steps outlined below and shown in Figure 1:

Form Team: A team is formed by selecting cross-functional resources consisting of personnel familiar with the various operational areas in your organization. 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 upon the skills and/or expertise required to complete the assessment process.

Select Standards: The CS^{2}SAT provides a list of security standards under the "navigation" tab within the tool. Based on the user's selections, the CS^{2}SAT generates questionnaires associated with these standards for use in the self-assessment process.

Determine Assurance Level: 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. The questionnaire assists an organization in determining the potential losses that could occur in terms of economic losses, death or injury, and environmental impacts. The CS^{2}SAT 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.

Figure 1: CS^{2}SAT Process Flow



Analyze Network Topology: The CS^{2}SAT contains a graphical user interface, which allows users to build the control system network topology (including criticality levels) into the CS^{2}SAT software. By creating an ICS network architecture diagram based upon components deemed critical to the organization, users are able to define the organizations cyber security boundary and posture. An icon palette is provided for the various system components allowing users to drag and drop components into a representative ICS architecture.

Answer Questions: CS^{2}SAT generates questions based on the specified network topology, the SAL, and the security standards which were selected. The assessment team then selects the best answer to each question based on their control system's configuration and implemented security practices. The CS^{2}SAT compares the answers provided by the assessment team with the recommended security standards and generates a list of security gaps.

Review Reports: The CS^{2}SAT generates reports in either the electronic or printed formats. The reports provide a summary of the answers which did not meet the recommendations of the selected standards. The assessment organization can then use this information to plan and prioritize mitigation strategies.

Self-Assessment Logistics and On-Site Visits

The CSSP can provide "over-the-shoulder" training and guidance to asset owners in using the CS^{2}SAT during on-site visits. To assist an organization in planning and organizing for an ICS assessment using the CS^{2}SAT, the following actions and items are recommended:

- Identify the assessment team members and schedule a date.
- Become familiar with information about their ICS in areas such as; polices and procedures, network topology diagrams, inventory list of critical control system assets and components, risk assessments, IT 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 on-site or subject matter support.

Typical DHS Control Systems Security Program On-Site Support

An example agenda for an on-site assistance visit from the CSSP would include the following activities:

1. **ICS Awareness Briefing** – 1 hour
   - Control system security awareness briefing
   - CS^{2}SAT 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 CSSP, visit:
http://www.US-CERT.gov/control_systems

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

To Report Cyber Incidents and Vulnerabilities

CSSP encourages you to report suspicious cyber activity, incidents, and vulnerabilities affecting critical infrastructure control systems. Online reporting forms are available at https://forms.us-cert.gov/report/. You can also submit reports via one of the following methods:

Phone: 1-888-282-0870
ICS related cyber activity: ics-cert@dhs.gov
General cyber activity: soc@us-cert.gov