Homeland Security

NCCIC
National Cybersecurity and Communications Integration Center

CYBER RESILIENCE REVIEW & CYBER SECURITY EVALUATION TOOL

The Department of Homeland Security's (DHS) Office of Cybersecurity & Communications (CS&C) conducts complimentary and voluntary assessments to evaluate operational resilience and cybersecurity capabilities within critical infrastructure sectors, as well as state, local, tribal, and territorial governments. The Cyber Security Evaluation Program (CSEP) administers the Cyber Resilience Review (CRR) while the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) offers the Cyber Security Evaluation Tool® (CSET) for industrial control systems. While related, the CRR and CSET are two distinct assessments with different areas of focus. Organizations should carefully review the information below and determine which assessment best fits their operating environment.

The inherent principles and recommended practices within the CRR and CSET align closely with the central tenets of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

CYBER RESILIENCE REVIEW

What is the CRR?

The CRR is a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities of an organization. The CRR is based on the CERT Resilience Management Model (http://www.cert.org/resilience/rmm.html), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience.

How Do Organizations Conduct a CRR?

Organizations have two options for conducting a CRR:

1. A free self-assessment download:

   www.us-cert.gov/ccubedvp/self-service-crr

2. An on-site facilitated session involving DHS representatives trained in the use of the CRR

What are the Benefits of Conducting a CRR?

Both options use the same assessment methodology and will lead to a variety of benefits, including:

- A better understanding of the organization's cybersecurity posture;
- An improved organization-wide awareness of the need for effective cybersecurity management;
- A review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crises;
- A verification of management success;
- An identification of cybersecurity improvement areas; and
- A catalyst for dialog between participants from different functional areas within an organization.

The CRR, whether through the self-assessment tool or facilitated session, will generate a report as a final product.

What Does the CRR Measure?

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness

How Do I Request a CRR?

To schedule a facilitated CRR or to request additional information please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov. To obtain the CRR self-assessment materials visit the webpage at www.us-cert.gov/ccubedvp/self-service-crr.

CYBER SECURITY EVALUATION TOOL

The Cyber Security Evaluation Tool (CSET®) provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture. It is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate their industrial control system (ICS) and information technology (IT) network security practices. Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations. The Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) developed the CSET application, and offers it at no cost to end users.

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

When the questionnaires are completed, CSET provides a dashboard of charts showing areas of strength and weakness, as well as a prioritized list of recommendations for increasing the sites cybersecurity posture. CSET includes recommendations, common practices, compensating actions, and suggested component enhancements or additions. CSET supports the capability to compare and merge and trend multiple assessments.

What are the Benefits of Using CSET?

- Provides a systematic, repeatable, and comparable method for assessing infrastructure
- Supports the capability to perform multiple assessments, and baseline and measure the results for comparison within future assessments
- Presents an analytic capability for determining design weaknesses or vulnerabilities, based upon importing a network diagram into the toolset
- Includes the capability to dynamically generate a network diagram to visualize the network infrastructure, including control system components and devices, as well as the ability to import a pre-built template diagram or import an existing MS Visio® diagram
- Houses a searchable resource library of reports, standards, templates, and white papers—for use in enhancing an organization's cyber security posture
- Provides enhanced reporting and output options, including an Executive Summary report, Site Summary report, or the capability to generate and create a customized System Security Plan (supporting output multiple formats such as MS Word or PDF) based upon the results of the assessment
- Incorporates video tutorials and self-help options for a guided approach to completing an assessment utilizing CSET.

How Do I Get Started?

Download CSET at: https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

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

About ICS-CERT

ICS-CERT works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors.

https://ics-cert.us-cert.gov

About NCCIC

The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

http://www.dhs.gov/national-cybersecurity-communications-integration-center