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.

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

WHAT DOES THE CRR MEASURE?

The CRR measures an organization's operational resilience capabilities through examining cybersecurity practices across ten domains:

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

WHO CAN PARTICIPATE?

The CRR seeks participation from a cross-functional team consisting of representatives from many offices within an organization. These representatives may include personnel with the following roles and responsibilities within the organization:

- **IT policy & procedures** (Chief Information Security Officer)
- **IT security planning & management** (Director of Information Technology)
- **IT infrastructure** (network or system administrator)
- **IT operations** (configuration/change manager)
- **Business operations** (operations manager)
- **Business continuity & disaster recovery planning** (BC/DR manager)
- **Risk analysis** (enterprise/operations risk manager)

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.

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.**

Homeland Security

CYBER SECURITY EVALUATION TOOL

WHAT IS THE CSET?

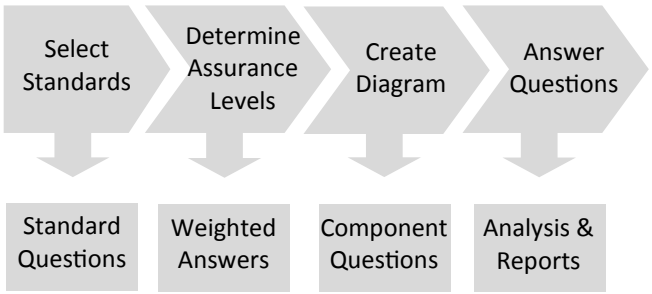
The CSET is a no-cost, voluntary technical assessment which provides a snapshot of an organization's cybersecurity posture. It helps asset owners and operators assess cybersecurity strengths and weaknesses within their control system environments and can also be used to assess traditional IT infrastructure.

The CSET exists as a downloadable application (free of charge), which can be installed locally on a standalone workstation or laptop. Once installed, the tool guides an asset owner through a step-by-step process to assess their environment, based upon a series of questions derived from industry recognized standards, guidelines, and best practices.

Once the questions are answered, CSET provides a graphical representation, identifying areas of strength and weakness, as well as a prioritized listing of options for increasing the organization's overall cybersecurity defense-in-depth.

WHAT ARE THE BENEFITS OF 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 a deep-dive 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 and visualization of the infrastructure, including control system components and devices;
- 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; and
- Incorporates video tutorials and self-help options for a guided approach to completing an assessment utilizing CSET.



Standards/Question Sets in CSET	Short Name
NIST Special Publication 800-53 Rev 3	800-53 R3
NIST Special Publication 800-53 Rev 3 App I	800-53 R3 App I
NIST Special Publication 800-53 Rev 4	800-53 R4
NIST Special Publication 800-53 Rev 4 App J	800-53 R4 App J
NIST Special Publication 800-82	SP800-82
NIST Special Publication 800-82 Rev 1	SP800-82 V1
NIST Special Publication 800-82 Rev 2 (Draft)	SP800-82 V2
Consensus Audit Guidelines (CAG)	CAG
Components Questions Set	Components
CFATS Risk-Based Performance Standards Guide 8-Cyber	CFATS
CNSSI No. 1253 Baseline	CNSSI 1253
CNSSI No. 1253 Industrial Control System (ICS) Overlay V1	CNSSI ICS
Catalog of Recommendations Rev 7	COR 7
DOD Instruction 8500.2	DOD 8500.2
INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	INGAA
Key Questions Set	Key
NIST Framework for Improving Critical Infrastructure Cybersecurity V1	NCSF V1
NEI 0809 Cyber Security Plan for Nuclear Power Reactors	NEI 0809
NERC CIP-002 through CIP-009 Rev 3	NERC Rev 3
NERC CIP-002 through CIP-009 Rev 4	NERC Rev 4
NISTIR 7628 Guidelines for Smart Grid Cyber Security: Vol. 1	NISTIR 7628
NRC Regulatory Guide 5.71	NRC 5.71
TSA Pipeline Security Guidelines April 2011	TSA
Universal Questions Set	Universal

HOW DO I GET STARTED?

Get started by downloading CSET at: **http://ics-cert.us-cert.gov/Downloading-and-Installing-CSET**. To learn more about CSET or to request a DVD copy of the software, contact **cset@dhs.gov**.

ABOUT THE ICS-CERT

The ICS-CERT, within DHS's National Protection and Programs Directorate's CS&C National Cybersecurity & Communications Integration Center 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, tribal, and territorial governments and control systems owners, operators, and vendors.