CYBER RESILIENCE REVIEW & CYBER SECURITY EVALUATION TOOL

The Cyber Security Evaluation Program and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) , within the Department of Homeland Security's (DHS) Office of Cybersecurity & Communications, conduct complimentary no-cost, voluntary, assessments (one non-technical and one technical) to evaluate operational resilience and cybersecurity capabilities within Critical Infrastructure sectors, as well as State, Local, Tribal, and Territorial governments through the Cyber Resilience Review (CRR) process and using the Cyber Security Evaluation Tool (CSET) for industrial control systems.

CYBER RESILIENCE REVIEW

The goal of the CRR is to develop an understanding of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. 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.

One of the foundational principles of the CRR is the idea that an organization deploys its assets (people, information, technology, and facilities) in support of specific operational missions (i.e., critical services). Applying this principle, the CRR seeks to understand an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors in the following 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

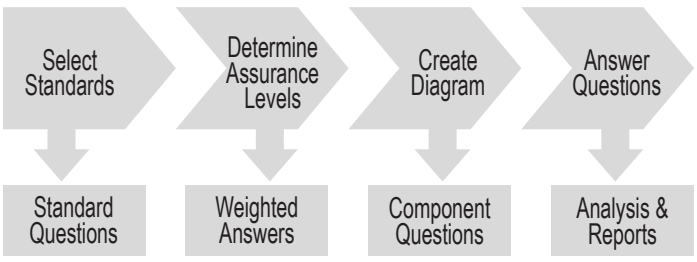
The CRR seeks participation from a cross-functional team consisting of representatives from business, operations, security, information technology, and maintenance areas

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. The CRR enables an organization to assess its capabilities relative to the CSF and a crosswalk document that maps the CRR to the NIST CSF is included as a component of the CRR self-assessment package. Though the CRR can be used to assess an organization's capabilities, the NIST CSF is based on a different underlying framework and as a result an organization's self-assessment of CRR practices and capabilities may fall short of or exceed corresponding practices and capabilities in the NIST CSF. Immediately after the NIST CSF was published, ICS-CERT began work incorporating the framework into the CSET tool. This integration is expected to be completed in the second half of 2014 while the tool continues to be a useful self-assessment for a cybersecurity baseline evaluations.

CYBERSECURITY EVALUATION TOOL

CSET helps asset owners 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 questions are answered, 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 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 configuration.



within an organization. These representatives may include personnel with the following roles and responsibilities within the organization:

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

HOW TO CONDUCT A CRR

Organizations have two options in conducting a CRR: a self-assessment available free for download from www.us-cert.gov/ccubedvp/self-service-crr or an on-site facilitated session involving DHS representatives trained in the use of the 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 REVIEW

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

CSET AT-A-GLANCE

Over the past few years, ICS-CERT has assisted with numerous on-site evaluations across the country and in all critical infrastructure sectors. In CY2013, ICS owners and operators downloaded more than 4,000 copies of CSET, and ICS-CERT helped perform 72 on-site evaluations. Sectors with the highest number of evaluations include: water and water treatment, energy, transportation, defense industrial base, nuclear reactors and materials & waste. The ICS-CERT observed that the most common vulnerabilities identified through CSET evaluations were inadequate control system inventory tracking, missing formal documentation, limited audit capabilities, inadequate event monitoring, open permissions and privileges, and missing access control restrictions. Other categories of vulnerabilities include 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 the organization's ICS system components, the complete list of assets including all operational hardware and components, and the 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: 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 DHS CYBER AND ICS-CERT

The Cyber Security Evaluation Program and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), within the Department of Homeland Security's (DHS) National Protection and Programs Directorate's Office of Cybersecurity and Communications and National Cybersecurity & Communications Integration Center (NCCIC), 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.