Homeland Security

Stakeholder Engagement and Critical Infrastructure Resilience

CYBER RESILIENCE REVIEW

The Cyber Security Evaluation program, within the Department of Homeland Security's (DHS) Office of Cybersecurity & Communications, conducts a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities within Critical Infrastructure and Key Resources sectors, as well as State, Local, Tribal, and Territorial governments through its Cyber Resilience Review (CRR) process.

OVERVIEW

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 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)

RELATIONSHIP TO THE NIST CYBERSECURITY FRAMEWORK

While the CRR predates the establishment of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), the inherent principles and recommended practices within the CRR 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.

Homeland Security

Stakeholder Engagement and Critical Infrastructure Resilience

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. The report contains each of the questions and answers contained within the assessment along with relevant options for consideration. These options for consideration are based on recognized standards, best practices, or references to the CERT Resilience Management Model. Additionally the final report contains an overall mapping of the relative maturity of the organizational resilience processes in each of the ten domains.

The CRR Report is for the organization's use and DHS does not share these results. The self-assessment does not collect any information; DHS uses information collected during the on-site assessment for anonymized data analytics only. This information is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/pcii].

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.