Homeland Security

Stakeholder Engagement and Cyber Infrastructure Resilience

CYBER RESILIENCE REVIEW

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

OVERVIEW

The goal of the CRR is to develop an understanding and measurement of key cybersecurity capabilities to provide meaningful indicators 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 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). To ensure the protection and sustainment of its critical services, 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. This is essential considering no one individual typically has the span of responsibility or knowledge to effectively address every CRR domain. These representatives can be personnel who have 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)

Homeland Security

Stakeholder Engagement and Cyber Infrastructure Resilience

WHAT TO EXPECT

The CRR is a one-day, on-site, facilitated interview of key cybersecurity personnel. Immediate on-site benefits may include:

- 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.

Participants will receive a draft CRR Report within 30 calendar days to review and provide feedback before a final CRR Report is issued to their organization. The report includes options for consideration that provide general guidance aimed at increasing an organization's cybersecurity posture and preparedness. This report may be used to support decision-making and help formulate cybersecurity investment justifications. The CRR Report is for the organization's use and DHS does not share these results. 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 CRR, or to request additional information, please email the Cyber Security Evaluation Program at CSE@hq.dhs.gov.

ABOUT DHS CYBER

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. As DHS's lead agency on cybersecurity, CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. For more information please visit www.dhs.gov/cyber.