About DHS and NCSD

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. NCSD leads DHS’s efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber.

CRR Domains & Asset Types

The CRR focuses on the following ten domains:

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

The CRR addresses the following four asset types:

1. People
2. Information
3. Technology
4. Facilities

What to Expect

- The CRR is a one-day, on-site facilitation and interview of key cyber security personnel.
- The participants will receive a draft report within 45 calendar days to review and provide feedback report results. DHS will subsequently issue a final CRR Report.
- CRR results are afforded protections under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/PCII] — the results are for organization use and DHS does not share results.

Contact Information for CRR-related Inquiries

Please address inquiries regarding the CRR to: CSE@hq.dhs.gov (Cyber Security Evaluations).

Overview

The CRR is based on the CERT Resilience Management Model (CERT-RMM) developed by Carnegie Mellon University’s Software Engineering Institute [www.cert.org/resilience/rmm.html].

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 and assets during normal operations and during times of operational stress and crises.

The CRR seeks to elicit the current state of cyber security management practices from key cyber security personnel, including those serving in the following roles:

- Chief Information Officers;
- Chief Information Security Officers;
- IT Security management;
- IT Operations management; and
- Business Continuity management.

Each participating organization will receive a CRR Report that includes findings in each domain and provides options for consideration containing general guidance or activities aimed at improving the cyber security posture and preparedness of an organization.