Homeland Security

CYBER RESILIENCE REVIEW

CYBER RESILIENCE REVIEW (CRR)

OVERVIEW

The Office of Cybersecurity and Communications National Cyber Security Division (NCSD), Cyber Security Evaluation Program (CSEP), has developed an assessment to measure and enhance the implementation of key cyber security capacities and capabilities of critical infrastructure and key resources (CIKR). The assessment, which is beneficial to all sectors of industry, is called the Cyber Resilience Review (CRR).

The objective of using the CRR at specific CIKR providers is to measure adoption and maturity aspects of cyber security risk management behaviors, using a common framework. The results can be used with regional studies to build a common perspective on Resilience, and to examine systems-of-systems (i.e., large and diverse operating and organizing models). The key goal of the CRR is to identify gaps and capabilities of cyber security management across all 18 critical infrastructure sectors. The evaluation scope includes an analysis of the cyber security management of assets that can profoundly affect our national prestige and morale, as well as can have a debilitating effect on public safety and economic well-being.

CYBER RESILIENCE REVIEW OF CIKR

A CRR is based on the CERT® Resilience Management Model, developed by the Software Engineering Institute at Carnegie Mellon University. The CRR examines cyber security management capabilities important to the identification and analysis of essential services and assets of CIKR, as well as management of cyber dependencies and interdependencies between CIKR. Topics discussed in the CRR include:

- Asset Definition and Management
- Communications Management
- Technology and Information Management
- Incident Management and Control
- Vulnerability Analysis and Resolution
- Environmental Control
- External Dependency
- Situational Awareness

Approximately 30 - 45 days following the CRR, participants receive a report from DHS that includes the results of the assessment, as well as recommended improvements to cyber security management practices based on any identified gaps.

WHAT TO EXPECT

- The interview-based assessment is in the form of a workshop with site personnel. Roles of participants typically include chief information officers, chief information security officers, IT systems and process control engineers, and business continuity personnel.
- The CRR takes approximately 4 to 6 hours to complete.
- Analyzed results will provide stakeholders with:
    - Options for consideration for improving cyber security in support of critical infrastructure operations
    - Documentation of capabilities and capacities to include strengths, weaknesses, and opportunities.

CONTACT INFORMATION FOR CRR-RELATED INQUIRIES

Please address inquiries regarding the CRR to:

CSE@hq.dhs.gov
Cyber Security Evaluations Program
National Cyber Security Division
Office of Cybersecurity and Communications