



## 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.

# STOP.THINK.CONNECT.™

## Stop.Think.Connect.™ Cyber Awareness Coalition

### OVERVIEW

Unlike other threats currently facing the country, cyber attacks can have instant, wide-ranging consequences for the nation's broader national and economic security interests. The targets of these attacks can vary – with some focusing on networks belonging to large organizations and others preying on individual Americans. Given this unprecedented and rapidly escalating threat, Federal agencies as well as State, local, tribal, and territorial (SLTT) governments must play a role in educating their employees and constituents to identify and deter online dangers. To make the Internet a safer place for all Americans, Federal agencies, and SLTT governments must share in the responsibility to promote heightened awareness about cybersecurity and safer online practices.

In an effort to encourage much needed Federal agency and SLTT government leadership on this important issue, the Department of Homeland Security's (DHS) Stop.Think.Connect. Campaign created the **Cyber Awareness Coalition**. The Coalition serves as an outlet for Federal agencies and SLTT governments to work directly with DHS and the Stop.Think.Connect. Campaign to promote awareness about cyber threats and online safety practices both within their organizations and to the general public.


### ADVANTAGES OF JOINING THE COALITION

By becoming a member of the Stop.Think.Connect. Cyber Awareness Coalition, your agency or SLTT government will have opportunities to demonstrate leadership on cybersecurity. Advantages of membership in the Coalition include the ability to:

- **Form productive and open relationships** with DHS, the National Cyber Security Alliance (NCSA), and other Federal, private, and non-profit Campaign stakeholders
- **Become a cybersecurity thought leader** by participating in monthly strategy conference calls with Stop.Think.Connect. leadership and stakeholders as well as distributing or contributing to Campaign cybersecurity materials, templates, resources, and tips
- **Enhance community involvement efforts** through participation in Stop.Think.Connect. Cyber Tours, which attract media attention and bring together communities to embrace a more sustained, proactive approach towards online safety
- **Demonstrate concern** for individuals, families, communities, and the country by working to deter vulnerabilities to online dangers



**Homeland  
Security**

  
STOP | THINK | CONNECT™