IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

DEFEND TODAY, SECURE TOMORROW

CYBER INFRASTRUCTURE SURVEY

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE CYBER INFRASTRUCTURE SURVEY (CIS) ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTED BY REGIONALLY-LOCATION CYBERSECURITY ADVISORS, A CIS EVALUATES THE EFFECTIVENESS, RESILIENCE AND CYBERSECURITY PREPAREDNESS OF AN ORGANIZATION'S SECURITY CONTROLS.

FORMAT AND GOAL

A CIS is a facilitated, expert-led assessment with cybersecurity personnel from your organization (e.g., Chief Information Security Officer, ICS/SCADA Security Manager, IT Security Manager). This informal interview typically takes 2½ to 4 hours in length.

Its goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify dependencies, capabilities and emerging effects of the current cybersecurity posture. After the survey, DHS will provide an interactive dashboard for scenario planning.

APPROACH

CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.

Following the assessment, DHS will provide a user friendly dashboard for reviewing and interacting with the survey findings. Your organization can use the dashboard to compare its results against its industry peers, review results in the context of specific cyber and physical threat scenarios, and dynamically adjust the importance of in-place practices to see the effects on overall cyber protection.

CYBERSECURITY FRAMEWORK

The cybersecurity controls surveyed within the CIS broadly align to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), but does not show an organization's adherence to the NIST CSF. The CIS computes a unique, service-specific cyber protective resilience index based on only a narrow set of cyber protection and resilience measures. The NIST CSF is a comprehensive framework and should be considered as a next step after leveraging the CIS results.

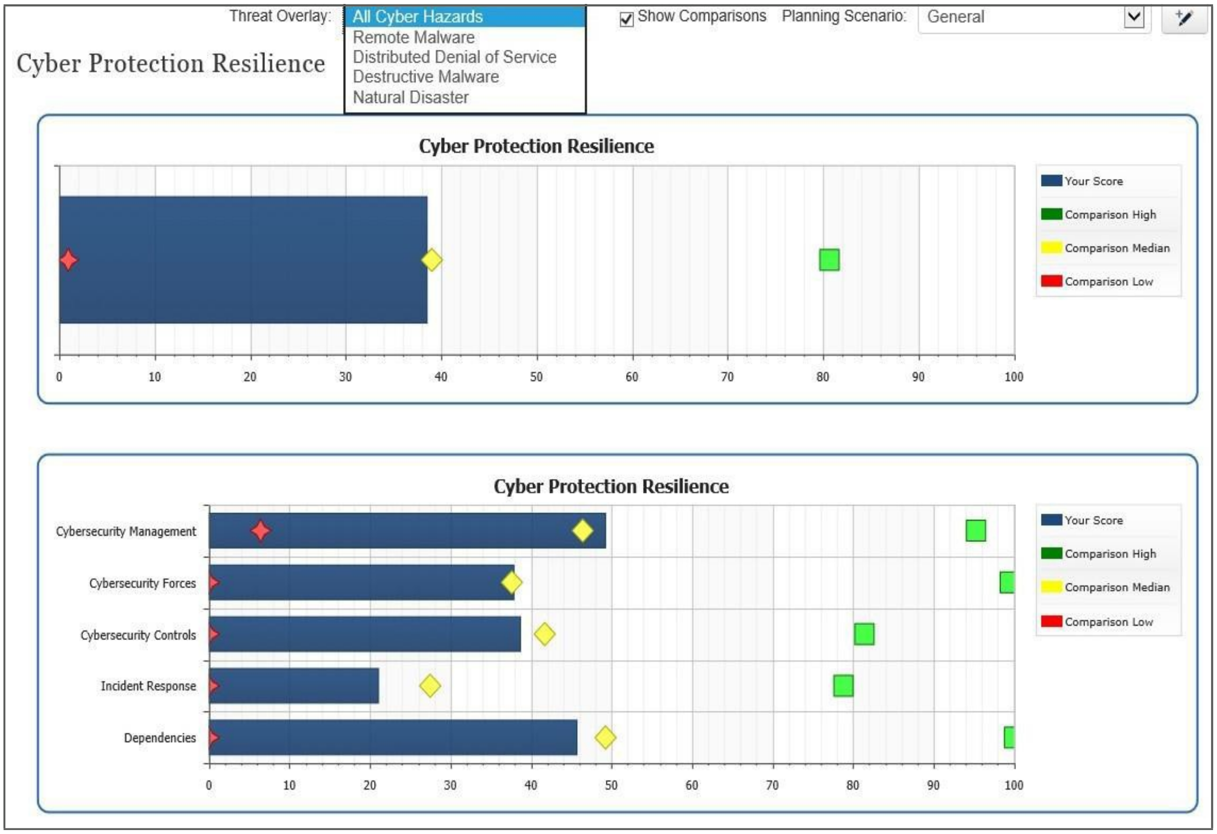
BENEFITS AND OUTCOMES

A CIS provides your organization with:

- An effective assessment of cybersecurity controls in-place for critical service;
- A user friendly, interactive dashboard to support cybersecurity planning and resource allocation; and
- Access to peer performance data, visually depicted on the dashboard.

DATA PRIVACY

The CIS dashboard is for your organization's exclusive use. All data collected and analysis performed during the CIS is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.



Cyber Protection Resilience

Threat Overlay: All Cyber Hazards

- All Cyber Hazards
- Remote Malware
- Distributed Denial of Service
- Destructive Malware
- Natural Disaster

☑ Show Comparisons

Planning Scenario: General

CIS Survey Question Domains

CIS Domains

Cybersecurity Forces

- Personnel
- Cybersecurity Training

Cybersecurity Controls

- Authentication and Authorization Controls
- Access Controls
- Cybersecurity Measures
- Information Protection
- User Training
- Defense Sophistication and Compensating Controls

Incident Response

- Incident Response Measures
- Alternate Site and Disaster Recovery

Cybersecurity Management

- Cybersecurity Leadership
- Cyber Service Architecture

- Change Management
- Lifecycle Tracking
- Assessment and Evaluation
- Cybersecurity Plan
- Cybersecurity Exercises
- Information Sharing

Dependencies

- Data at Rest
- Data in Motion
- Data in Process
- End Point Systems

For further information, contact your Cybersecurity Advisor (CSA) at iodregionaloperations@cisa.dhs.gov.