# CYBER INFRASTRUCTURE SURVEY TOOL (C-IST)

The Department of Homeland Security (DHS) Office of Cybersecurity & Communications (CS&C) conducts a no-cost, voluntary assessment to evaluate controls-based cyber protection and resilience measures within critical infrastructure sectors, as well as State, Local, Tribal, and Territorial governments through the Cyber Infrastructure Survey Tool (C-IST).

## OVERVIEW

The C-IST is an assessment of essential cybersecurity practices in-place for critical services within critical infrastructure organizations. The C-IST is a structured, interview-based assessment focusing on over 80 cybersecurity controls grouped under five key surveyed topics. Following the assessment, DHS provides participants with the ability to review and interact with the surveyed findings through a user-friendly, data-rich dashboard.

The C-IST dashboard allows organizations to see their results compared against other members of their critical infrastructure sectors, review their results in context of specific cyber and physical threat scenarios, and dynamically adjust the status of in-place practices to see the effects on overall cyber protection.

The key principles of the C-IST method focus on protective measures, threat scenarios, and a service-based view of cybersecurity in the context of the following five surveyed topics:

1. Cybersecurity Management
2. Cybersecurity Forces
3. Cybersecurity Controls
4. Cyber Incident Response
5. Cyber Dependencies

The C-IST is a facilitated, expert-led assessment accomplished through an informal interview (typically over the course of 2 ½ to 4 hours) with one to two cybersecurity personnel within an organization.

These personnel may serve in the following roles and responsibilities within the organization:

- Chief Information Security Officer
- ICS/SCADA Security Manager
- IT Security Manager

## BENEFITS

The C-IST provides various benefits to an organization, including:

- An effective, repeatable assessment of cyber security controls in-place for a critical service within public and private sector organizations
- A user-friendly, interactive dashboard to support cybersecurity planning and resource allocation
- Context-rich information with peer comparison where peer data is available

The C-IST dashboard is for the organization's exclusive use and DHS has strict provisions for sharing anonymized, surveyed results with approved partner organizations. All data collected and analysis performed under the C-IST is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program [www.dhs.gov/pcii].

## RELATIONSHIP TO THE CYBERSECURITY FRAMEWORK

The cybersecurity controls surveyed within the C-IST broadly align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), however the C-IST should not be considered a survey of the NIST CSF. The C-IST comprises only a narrow set of cyber protection and resilience measures used to compute a unique, service-specific cyber protective index.

The NIST CSF is based on a different underlying framework, and as a result an organization's C-IST findings, may fall short of corresponding practices and capabilities in the NIST CSF.

## HOW DO I REQUEST A C-IST?

To schedule a C-IST or to request additional information, please email **cyberadvisor@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. DHS 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**.