



Purpose

The Cyber Infrastructure Survey Tool (C-IST) provides public and private sector organizations with an effective, repeatable survey of cyber security controls; the means to review their results as compared against peer organizations; and a user-friendly, interactive dashboard for planning improvements to critical IT services.

The C-IST is a facilitated evaluation performed with IT security personnel (e.g., CISO, ICS/SCADA Security Manager, Security Operations personnel, and Business Continuity / Incident Response personnel), accomplished through an informal interview with at least one participant over the course of 2 ½ to 4 hours.

The C-IST is intended to assist State, local, tribal, territorial (SLTT) government and private sector participants in surveying cyber protection and resilience measures in the following areas:

1. **CYBERSECURITY MANAGEMENT**
2. **CYBERSECURITY FORCES**
3. **CYBERSECURITY CONTROLS**
4. **INCIDENT RESPONSE & CONTINUITY**
5. **CYBER DEPENDENCIES**

Methodology

The C-IST methodology is based on decision analysis concepts and relies upon a perspective of protecting key information technology and/or operations technology *services*.

The key principles of the C-IST method focus on protective measures, threat scenarios, and a service-based view of cyber security. Critical infrastructure owners will find that results provide an easy to understand comparative analysis that compares cyber security based on similar operations environments and services.

Cyber IST Highlights

Primary Objectives

- Identifies (i.e., surveys) and reports (i.e., dashboards) cyber security information related to critical IT services
- Provides an interactive tool to support cybersecurity planning and resource allocation
- Provides peer comparisons and context-rich decision support information
- Assists security managers with establishing a baseline for measuring year-to-year progress

Key Features and Functions

- **Low Effort:** Lightweight questionnaire, performed over 2 ½ to 4 hours with a small number of organization personnel, and typically 1-2 personnel
- **Formal Deliverable:** Interactive dashboard, either Web-based or free-standing
- **Supports Program Planning:** Built-in trade-off analysis reflecting gains and losses in relative protection and resilience
- **Survey Data Protections:** Data collected and handled as Protected Critical Infrastructure Information (PCII)
- **Broad Applicability:** Applies to an organization within the 16 critical infrastructure sectors and SLTT government, and consistent with EO 13636 Cyber Security Framework (CSF)
- **Focuses on Critical Operations:** Data collection on critical services
- **Expert-Led:** Data collected by trained DHS personnel during onsite visit

Contact Information

To arrange a C-IST survey or for information inquiries, please contact:

cyberadvisor@hq.dhs.gov