CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ADVISORS

THE CYBERSECURITY AND INFRASTRUCTURE AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBERSECURITY ASSISTANCE ON A VOLUNTARY, NO-COST BASIS TO CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS. THROUGH THE CSA PROGRAM, YOUR ORGANIZATION CAN PREPARE FOR AND PROTECT AGAINST CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE.

GOALS

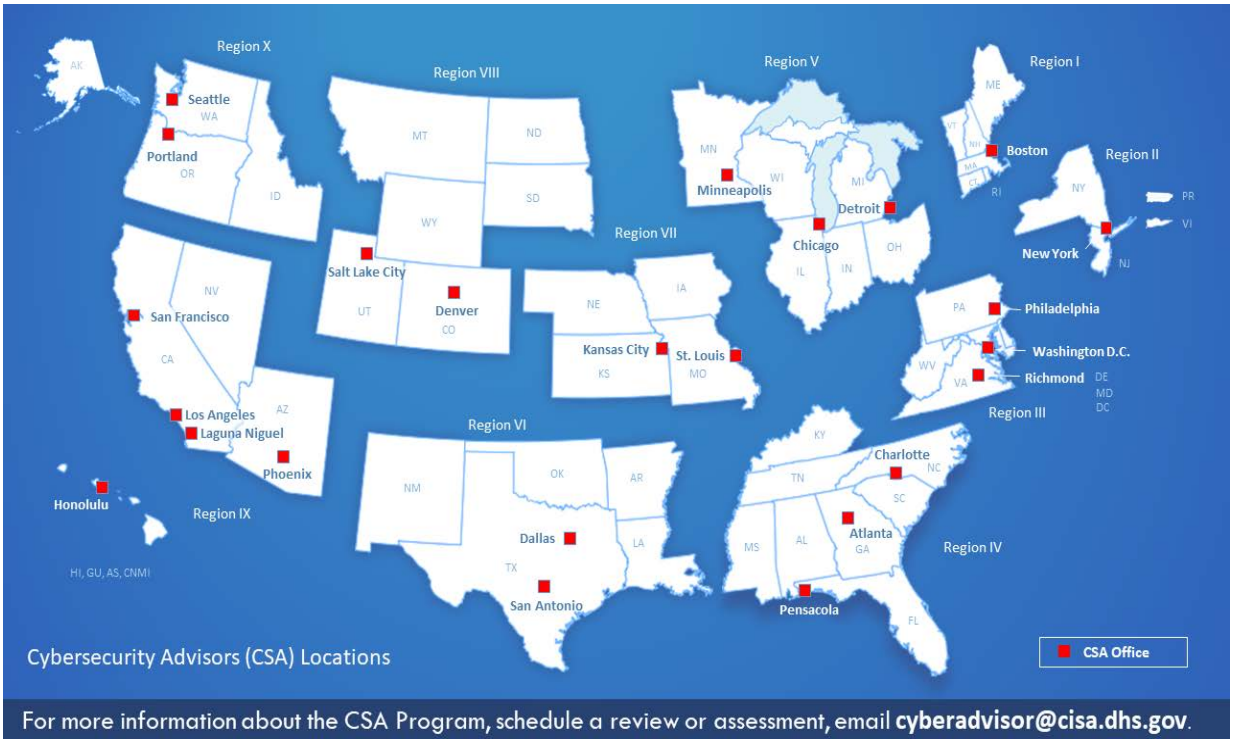
The goal of the CSA program is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure, as well as SLTT bodies, through stakeholder partnerships and direct assistance activities.

APPROACH

The CSA program maintains regional subject matter experts throughout DHS emergency management and protection regions. Regional CSAs cultivate partnerships with participating organizations and initiate information sharing. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership. CSAs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the United States.

Service	What CSAs Offer	What Value Our Partners Receive
Cyber Preparedness	On-site preparedness and protective visits, work- shops, and engaging activities	Cybersecurity ideas, advice, and best practices and a formal exchange to raise awareness of DHS cybersecurity products, services, and information resources relative to critical infrastructure and partnerships
Strategic Messaging	DHS cybersecurity briefings, keynote addresses, and panel discussions	Improved cybersecurity awareness and collaboration potential, to convey timely and relevant information on DHS programs and operational activities
Working Group Support	Leadership at existing forums and working groups, engaging stakeholders with in-place cybersecurity initiatives and information sharing groups	Improved coordination with DHS on cybersecurity policy, procedures, and best practices; and an opportunity to exchange lessons-learned and identify areas of mutual interest
Partnership Development	Engagements to develop, build capacity in, and strengthen private-public cybersecurity partner- ships	Help initiating cybersecurity partnerships, establishing charter objectives and milestones, and maturing local and regional cybersecurity posture — in order to move partnerships from awareness building to operational capabilities

Cyber Assessments	Cyber Infrastructure Survey (CIS)	Assessment of more than 80 cybersecurity controls in five domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies, resulting in an interactive decision support tool
	Cyber Resilience Review (CRR)	Assessment of cybersecurity management capabilities and maturity aspects of an organization's critical information technology (IT) services and associated assets — and in the context of the NIST Cybersecurity Frame- work (CSF)
	External Dependency Management (EDM)	Assessments of management activities and practices used to identify, analyze, and reduce risks arising from third parties
Incident Coordination and Support	Direct assistance and resourcing support, con- ducted in times of cyber threat, disruption, and attack	Facilitated cyber incident response and resource coordination, information de-confliction, and information request assistance



CYBER RESILIENCE REVIEW

THE PRESIDENTIAL POLICY DIRECTIVE (PPD) 41, UNITED STATES CYBER INCIDENT COORDINATION, SETS FORTH THE PRINCIPLES GOVERNING THE FEDERAL GOVERNMENT'S RESPONSE TO CYBER INCIDENTS AND ESTABLISHES LEAD AGENCIES AND PLANS FOR COORDINATING THE BROADER FEDERAL GOVERNMENT RESPONSE FOR THE AFFECTED ENTITIES, OR VICTIMS, OF SUCH INCIDENTS.

FORMAT AND GOAL

CISA offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your locations.

Through the CRR, the organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.

APPROACH

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring and defining cybersecurity capabilities across 10 domains:

- Asset Management,
- Controls Management,
- Configuration and Change Management,
- Vulnerability Management,
- Incident Management,
- Service Continuity Management,
- Risk Management,
- External Dependencies Management,
- Training and Awareness, and
- Situational Awareness.

PARTICIPANTS

To conduct a CRR, CISA recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)

- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERTRMM.

DATA PRIVACY

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment 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.

ASSOCIATION TO THE CYBERSECURITY FRAMEWORK

The principles and recommended practices within the CRR align with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and, where appropriate, recommended improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

CISA
CYBER+INFRASTRUCTURE

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.

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

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE EXTERNAL DEPENDENCIES MANAGEMENT (EDM) ASSESSMENT ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGAIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTERED BY REGIONALLY-LOCATED CYBERSECURITY ADVISORS, THE ASSESSMENT PROVIDES AN ORGANIZATION WITH A BETTER UNDERSTANDING OF HOW THEY MANAGE RISKS ARISING FROM DEPENDENCES ON THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN.

FORMAT AND GOALS

The EDM Assessment is conducted as a four-hour session at a location of your choosing and facilitated by trained DHS representatives. Your organization can use the assessment by itself and as the first step in an improvement effort. You also may use it in conjunction with CISA's External Dependencies Management Method, which provides a rigorous, repeatable way to identify and manage specific suppliers or other external entities that your organization depends on to support its mission.

The goals of the assessment are to:

- Evaluate the activities and practices your organization uses to manage risks arising from external dependencies.
- Provide an objective review of your organization's capabilities in the assessed areas and recommendations offering a roadmap for improvement based on industry-leading practices.

APPROACH

Risks associated with the ICT supply chain have grown dramatically with expanded outsourcing of technology and infrastructure. Failures in managing these risks have resulted in incidents affecting millions of people.

The EDM Assessment focuses on the relationship between your organization's high-value services and assets (people, technology, facilities, and information) and evaluates how you manage risks incurred from using the ICT supply chain to support these high-value services. The ICT supply chain consists of outside parties that operate, provide, or support information and communications technology. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT.

Through the EDM Assessment, your organization will evaluate:

- Relationship Formation – how your organization considers third-party risks, selects external entities, and forms relationships with them so that risk is managed from the start.
- Relationship Management and Governance – how your organization manages ongoing relationships with external entities to support and strengthen your critical services at a managed level of risk and costs.

- Service Protection and Sustainment – how your organization plans for, anticipates, and manages disruption or incidents related to external entities.

The EDM Assessment evolved from the DHS Cyber Resilience Review (CRR) and, like the CRR, is based on the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute.

BENEFITS AND OUTCOMES

Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies. The assessment provides:

- An opportunity for participants from different parts of you organization to discuss issues relating to vendors and reliance on external entities;
- Options for consideration that guide improvement efforts, using recognized standards and best practices drawn from such sources as the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework; and
- A comprehensive report on your third-party risk management practices and capabilities.

DATA PRIVACY

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

PARTICIPANTS

To conduct an EDM assessment, CISA recommends that you involve a cross-functional team that includes those responsible for the functions shown in the following.

- IT security planning and management (e.g., Director of Information Technology)
- IT operations (e.g., configuration/change managers)
- Risk managers, in particular operations risk (e.g., enterprise/operations risk manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- IT policy and governance (e.g., Chief Information Security Officer)
- Business management (e.g., operations manager)
- Procurement and vendor management (e.g., contracts and legal support managers)
- Legal

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER RESILIENCE WORKSHOP

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBER RESILIENCE WORKSHOPS ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. THROUGH THE WORKSHOP, YOUR ORGANIZATION WILL BE INTRODUCED TO CYBER RESILIENCE CONCEPTS AND WAYS TO IMPROVE MANAGEMENT OF CYBER RESILIENCE.

FORMAT

The Cyber Resilience Workshop is a four-hour collaborative session led by CISA representatives. Each workshop is tailored to the concerns and threats of a specific sector and provides an opportunity for professionals to learn together. Workshops are held on demand (based on availability) at locations convenient to participants.

GOAL

The goal of the workshop is to provide your organization with tangible, useful take-away information related to risk-based decision making and security planning for critical services.

APPROACH

Through the workshop, your organization will be introduced to cyber resilience concepts and capability-building activities in key performance areas such as cybersecurity, IT operations, and business continuity. The workshop will address both operational risk management and emergency/crisis management. Structured drills and scenarios will help your organization examine capability building in operational resilience practices, going well beyond discussions of IT security controls and countermeasures. Content and threat examples specific to your sector or industry will be emphasized.

PARTICIPANTS

CISA recommends that a cross-functional team from your organization's business and operations attend the workshop, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)
- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The Cyber Resilience Workshop is designed to keep communities-of-interest informed on national cybersecurity, policies, initiatives, and federal capabilities, and to encourage working partnerships with these communities on matters of cybersecurity. The workshop will provide your organization with a greater awareness of:

- Federal initiatives affecting critical infrastructure protection and realistic practices for improving operational resilience;
- Gaps in cyber management practices and potential process improvements;
- Cybersecurity best practices and operational resilience concepts;
- Processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services;
- Ways to enhance cyber incident response and business continuity capabilities; and
- Federal coordination for incident notification, containment, and recovery.

FOR INFORMATION AND SCHEDULING

The Cyber Resilience Workshop is facilitated by regional personnel of the Cybersecurity Advisor (CSA) Program. Email cyberadvisor@hq.dhs.gov for more information on the Cyber Resilience Workshop and on the schedules and locations of upcoming sessions.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Cyber Resilience Review (CRR)	External Dependency Management (EDM)	Cyber Infrastructure Survey (CIS)	Onsite Cyber Security Evaluation Tool (CSET)
Purpose and Value Proposition	Identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.	Assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.	Identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.	Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance
Scope	Critical Service view	Critical Service view	Critical Service view	Information Technology and Operational Technology systems
Time to Execute/	5 to 6 Hours	3 – 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours) (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Capabilities and maturity indicators across third party relationship management lifecycle domains	Protective measures in-place	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Planning call to scope evaluation	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager, Continuity Planner, with Contract Management	IT/Security Manager	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts
All Assessments Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services			