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.

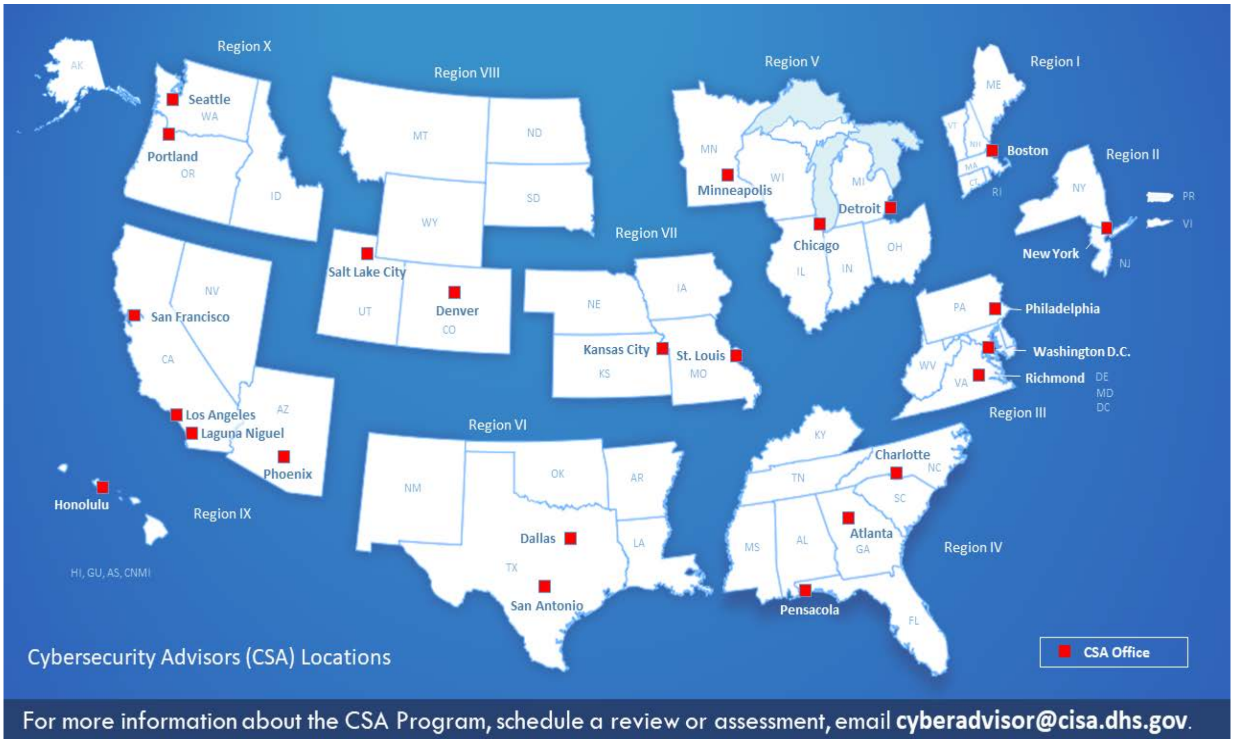
APPROACH

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

2019-09-13

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



Cybersecurity Advisors (CSA) Locations

For more information about the CSA Program, schedule a review or assessment, email **cyberadvisor@cisa.dhs.gov**.