CYBERSECURITY ADVISORS

The Department of Homeland Security's (DHS) Cybersecurity Advisors (CSAs) offer assistance to help prepare and protect private sector entities and state, local, territorial, and tribal (SLTT) governments from cybersecurity threats. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities.

CSAs are distributed personnel assigned to 10 regions throughout the U.S., which are aligned to the Federal Emergency Management Agency (FEMA) regions. CSAs *are where the partners are* - engaging to cultivate partnerships, to deliver cybersecurity services, and to direct feedback and facilitate inquiry seamlessly to DHS cyber programs and Department leadership.

CSA SERVICES

Cybersecurity Advisors offer six types of services:

1. **Cyber Preparedness:** On-site meetings to answer questions, exchange ideas and information, and address concerns about cybersecurity — promoting best practices, resources, and partnership experiences.
2. **Strategic Messaging:** Briefings, keynotes, and panel discussions delivered to help improve cybersecurity awareness and organizations' cybersecurity posture — including timely and relevant information on DHS programs and operational activities.
4. **Working Group Support:** Engagements to join stakeholders in existing cybersecurity initiatives and groups to enhance information sharing — improving policy, procedures, and best practice, and facilitating lessons-learned.
5. **Partnership Development:** Engagements to build and mature local and regional cybersecurity private-public partnerships, and move partnerships from awareness building to operational capabilities.

5. **Cyber Assessments:**
   - **Cyber Infrastructure Survey Tool (C-IST):** Survey focused on over 80 cybersecurity controls in five key areas, resulting in an interactive decision support tool.
   - **Cyber Resilience Review (CRR):** Strategic evaluation that assesses cybersecurity management capabilities and maturity as applied to protect critical information technology (IT) services.
   - **External Dependency Management (EDM):** Assessment of the management activities and practices utilized to identify, analyze, and reduce risks arising from third parties.
6. **Incident Coordination and Support:** Activities to facilitate cyber incident response and to coordinate information requests in times of increased threat, disruption, and attack.

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 on DHS cyber programs, visit www.dhs.gov/cyber.