Homeland Security

MANAGING CYBER RISK

In conjunction with partners, DHS engages with SLTT representatives and the public to help enhance their cybersecurity risk postures and collaborates with them to leverage free resources available to improve their cybersecurity.

The Cyber Resilience Review (CRR), may be conducted as a self-assessment or in-person interview at no-cost, and examines the resilience of an organization's cybersecurity program through its policies and procedures. This review is based on the CERT Resilience Management Model and aligns with NIST's Cybersecurity Framework. It seeks to understand the key capabilities needed to improve an organization's cybersecurity risk management posture.

The Cyber Hygiene (CH) assessment is a no-cost, voluntary, technical assessment encompassing configuration error and vulnerability scanning. Based on findings, DHS offers recommendations on remediating and mitigating the vulnerabilities. This assessment is conducted remotely and on a specified recurring basis.

The Risk and Vulnerability Assessment (RVA) is a more in-depth no-cost, voluntary, technical assessment than Cyber Hygiene; This suite of services includes penetration testing, social engineering, wireless access discovery and identification, as well as database and operating system scanning.

The Continuous Diagnostics and Mitigation (CDM) program provides a consistent set of continuous monitoring solutions to enhance the ability of federal, State, local, tribal, and territorial government entities to identify and mitigate the impact of emerging cyber threats. DHS, in partnership with the General Services Administration (GSA), established a government-wide acquisition vehicle (blanket purchase agreement) that can be leveraged by SLTT governments to purchase services at the same discount available to federal customers.

The National Cyber Exercise and Planning Program (NCEPP) improves the Nation's cybersecurity readiness, protection, and incident response capabilities by developing, designing, and conducting cyber exercises and workshops at the SLTT, federal, regional, and international level. The cyber exercise team employs scenario-based exercises that focus on risks to cyber and information technology infrastructure. Through exercises, participants are able to validate policies, plans, procedures, processes, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations.

Cyber Security Advisors (CSA) are regionally located personnel that provide immediate and sustained assistance, coordination, and outreach to prepare and protect both SLTT and private sector critical infrastructure entities from cyber threats. CSAs bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of these entities and bring them into closer alignment with the Federal Government.

The SLTT Security Clearance Initiative grants security clearances to state CIOs and CISOs. These clearances enable CIOs and CISOs to receive actionable and valuable classified and sensitive information about current and recent cyber incidents and threats to better inform their cybersecurity risk management decisions.

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: www.dhs.gov/cyber.

To learn more about SLTT resources, email SLTTCyber@hq.dhs.gov.

Homeland Security

STATE, LOCAL, TRIBAL, AND TERRITORIAL CYBERSECURITY ENGAGEMENT

The Department of Homeland Security's (DHS) State, Local, Tribal and Territorial (SLTT) Cybersecurity Engagement program was established to help non-federal public stakeholders and associations manage cyber risk. The program provides appointed and elected SLTT government officials with cybersecurity risk briefings, and information on available resources, and partnership opportunities to help protect their citizens online. The program coordinates the Department's cybersecurity efforts with its SLTT partners to enhance and protect their cyber interests.

BUILDING A COMMUNITY TO PROMOTE A SHARED RESPONSIBILITY

To build trusted relationships, the SLTT program partners with stakeholders on all levels, and plans and coordinates cyber summits. The summits bring key stakeholders together to share best practices, discuss trends and advancements in the field, and foster public-private partnerships.

The STOP.THINK.CONNECT.™ Campaign and **National Cyber Security Awareness Month** in October are national cybersecurity awareness campaigns aimed at raising awareness for safe cyber practices among the American public. State and local participants can access campaign materials, templates, resources, and tips to assist with promoting cybersecurity within their communities. Visit www.dhs.gov/stopthinkconnect.

DHS's **Critical Infrastructure Cyber Community Voluntary Program (C³VP)** is the coordination point within the Federal Government to leverage and enhance existing capabilities to support use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a risk-based approach to cybersecurity strategy and policy.

INFORMATION SHARING

Close working relationships with key SLTT stakeholders are critical to fulfilling DHS's mission to protect the Nation's critical cyber infrastructure.

The DHS National Cybersecurity and Communications Integration Center (NCCIC) is a 24X7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement.

The NCCIC leads the protection of the federal civilian agencies in cyberspace, provides support and expertise to critical infrastructure owners and operators, and works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide expertise and information to SLTT governments.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is grant-funded and designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the Nation's SLTT governments. The MS-ISAC provides advisories, newsletters, cybersecurity guides and toolkits, working groups, monthly calls and many more services to all members in an effort to enhance cyber situational awareness.

Through its 24X7 Security Operations Center (SOC), the MS-ISAC serves as a central resource for situational awareness and incident response for SLTT governments while sharing and coordinating real-time risk information to support national cybersecurity situational awareness with DHS. The SOC provides real-time network monitoring, dissemination of early cyber threat warnings, and vulnerability identification and mitigation to reduce risk to the Nation's SLTT government cyber domain. Membership is free.