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 manage cyber risk. The program coordinates the Department's cybersecurity efforts with its SLTT partners to enhance and protect their cyber interests.

BUILDING A COMMUNITY OF 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 and discuss trends and advancements in the field.

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 and 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 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, 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. The SOC provides real-time network monitoring, dissemination of early cyber threat warnings, and vulnerability identification and mitigation to reduce cyber risks to SLTT governments. Membership is free.

MANAGING CYBER RISK

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

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 the vulnerabilities. This assessment is conducted remotely and on a 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.

Cyber Security Advisors (CSA) and Protective Security Advisors (PSA) 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 and physical threats.

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.

For more information: www.dhs.gov/cyber.

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