EIS Communiqué

Sharing Election Infrastructure News and Resources

February 7, 2018 Volume 1, Issue 4

Cybersecurity Advisors Are Here to Help

DHS's National Protection and Programs Directorate (NPPD) offers the **Cybersecurity Advisor (CSA) Program** which **provides cybersecurity assistance on a voluntary, no-cost basis to** critical infrastructure organizations, including **state, local, tribal, and territorial (SLTT) governments**. Through the CSA Program, state and local election officials can prepare for and protect against cybersecurity threats to election infrastructure.

The purpose of the CSA Program is to promote cybersecurity preparedness, risk mitigation strategies, and incident response capabilities for public and private sector owners and operators of critical infrastructure and SLTT entities.

CSAs build and strengthen public-private cybersecurity partnerships through on-site preparedness meetings and cyber protective visits. They address stakeholder needs by engaging in various working groups, tabletop exercises, and other technical exchanges. **CSAs are located throughout the United States**, and are available to perform risk-based cybersecurity assessments, such as the External Dependencies Management (EDM) Assessment, Cyber Infrastructure Survey (CIS), the Cyber Resilience Review (CRR), and the Cyber Security Evaluation Tool (CSET).

Fortifying Election Infrastructure Resiliency

The **Cyber Resilience Review** (CRR) is a no-cost, voluntary assessment intended to evaluate an entity's operational resilience and cybersecurity practices **to help increase resilience and continuity of critical services**. Through the CRR, an organization will develop an understanding and measure cyber security capabilities as they relate to operational resilience and cyber risk.

The CRR is based on the premise that an **organization deploys assets** --- people, information, technology, and facilities --- **to support specific critical services or products**. With that principle, the CRR evaluates the maturity of an organization's capacities and capabilities in performing, planning, managing and measuring, and defining cybersecurity across 10 domains:

1. Asset Management;
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependency Management
9. Training and Awareness
10. Situational Awareness.

CRR Benefits:

- Better understanding of one's cybersecurity posture;
- Improved organization-wide awareness of the need for effective cybersecurity management; and
- Review of capabilities most important to ensuring continuity of critical services during times of operational stress and crisis.

A CRR assessment can be self-administered or facilitated in one business day. Scheduling an assessment takes about two weeks. A comprehensive final report is provided to the organization about 30 days after the assessment. The final report maps the relative maturity of the organizational resilience processes to each of the 10 domains, and includes improvement options for consideration and best practices. For more information or to schedule an assessment, contact cyberadvisor@hq.dhs.gov or visit www.us-cert.gov/ccubedvp/assessments.

EIS Background

The Department of Homeland Security (DHS) designated election infrastructure as critical infrastructure on January 6, 2017. The designation created the Election Infrastructure Subsector under the Government Facilities sector, with DHS as its Sector Specific Agency (SSA). The designation set several actions in motion, such as the formation of coordinating councils, coordinated federal support, and the availability of services and tools for the Election Infrastructure Subsector. For more information on the topics of this Communiqué, please contact the EISSA at EISSA@hq.dhs.gov.

Purpose

The EIS Communiqué series will periodically inform subscribers of the myriad of Department of Homeland Security (DHS) services available to the EI community. DHS provides services on a no-cost, voluntary basis to state and local election officials.

Future EIS Communiqués will highlight various services and tools, such as assessments, threat information-sharing programs, network protection, best practices, incident response, and developments at the federal level.

Thank you,

Election Infrastructure SSA

We want to hear from you! Send us your comments on how we may better serve you as well as questions, feedback, and ideas for future Communiqué topics at EISSA@hq.dhs.gov.

Subscriber Services

Click here to subscribe Click here to unsubscribe