EIS Communiqué

Sharing Election Infrastructure News and Resources

Welcome to the DHS Election Infrastructure Subsector (EIS) Communiqué, provided by the Election Infrastructure Sector Specific Agency (EISSA). 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.

Purpose

The EIS Communiqué series will periodically inform subscribers of the myriad of 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.

Please share this Communiqué as widely as you wish. We look forward to receiving questions, feedback, and suggestions for future Communiqué topics at EISSA@hq.dhs.gov.

Thank you,

Election Infrastructure SSA

January 31, 2018 Volume 1, Issue 3

Assessing Risks, Vulnerabilities, and Threats Strengthens Defense

Internet-facing election systems on information technology networks can be vulnerable to a multitude of cyber threats. System and network assessments are invaluable to identify and mitigate vulnerabilities in order to thwart potential attacks.

A **Risk and Vulnerability Assessment (RVA)** is a no-cost offering that **combines national threat and vulnerability information** with data discovered through **onsite assessment activities** to provide stakeholders with **actionable remediation recommendations** prioritized by risk.

RVAs are designed to determine whether and by what means adversaries can defeat network security controls. Assessment elements include scenario-based network

penetration testing, web applications testing, social engineering testing, wireless testing, configuration reviews of servers and databases, and evaluation of an organization's detection and response capabilities.

Approximately two weeks after the assessment, stakeholders receive an **RVA Final Report** with business executive recommendations, specific findings, and potential mitigation steps, along with technical attack path findings. Stakeholders may also request an optional **RVA Outbrief** presentation at the end of the testing, which covers preliminary findings and observations, tailored to technical staff or business executives as requested.

Assessment duration typically takes two weeks: one week offsite and one week on-site. A point-of-contact is required and minimal IT support is needed to assist with issues such as connectivity and test accounts. There is typically a 90-day waiting list for an RVA.

Phishing Campaign Assessment Informs and Guides

The Phishing Campaign Assessment (PCA) is a no-cost, six-week engagement offered to federal, state, local, tribal, and territorial governments, as well as critical infrastructure and private sector companies. A PCA evaluates an organization's susceptibility and reaction to phishing emails. **Results** of a PCA are meant to **provide guidance, measure effectiveness, and justify resources** needed to defend against spear-phishing and increase user training and awareness.

Two weeks after the assessment, organizations receive a **PCA Report**, highlighting organizational click rates for various types of phishing emails and summarizes metrics related to the proclivity of an organization to fall victim to phishing attacks.

DHS's **National Cybersecurity Assessments and Technical Services (NCATS) Team** conducts both the Risk and Vulnerability Assessment and the Phishing Campaign Assessment. For more information on either assessment or to get started, contact nccicustomerservice@hq.dhs.gov.

For more information on any topic in this Communiqué, please contact the EISSA at EISSA@hq.dhs.gov.