EIS Communiqué

Sharing Election Infrastructure News and Resources

February 21, 2018 Volume 1, Issue 6

State Election Officials Meet for DHS Threat and Product Briefings

State election and federal officials met last week in Washington, D.C. to further fortify the foundation of collaboration, governance, information sharing, and risk mitigation to better secure the Nation's election infrastructure.

DHS Secretary Kirstjen Nielsen met last week with the **National Association of Secretaries of State (NASS) Executive Board** and discussed DHS's commitment to working with state election officials on cybersecurity for the midterm elections and beyond. In addition, **DHS, Office of the Director of National Intelligence, and the Federal Bureau of Investigation sponsored classified briefings for election officials from across the country**. Briefings focused on increasing awareness of foreign adversary intent and capabilities against the states' election infrastructure, and included a discussion of threat mitigation efforts including hunting for intruders in systems **(see discussion below for DHS hunt capabilities for election officials)**. For more information, see Readout DHS State Election Officials Meeting.

Hunting for Malicious Activity

DHS's National Protection and Programs Directorate (NPPD) provides expert intrusion analysis and mitigation guidance to stakeholders who lack the ability in-house to respond to a cyber incident or could use additional assistance through the **Hunt and Incident Response Team (HIRT)**. Based in NPPD's 24-7 National Cybersecurity and Communications Integration Center, HIRT supports federal, state, local, tribal, and territorial governments, critical infrastructure owners and operators, academia, and international organizations.

HIRT responds to cybersecurity incidents both onsite and from remote locations. Typical engagements include a log review, network traffic analysis, and a host analysis. The goal is to discover malicious actors, acquire and analyze the malicious tools, and provide mitigation guidance. HIRT searches for exploitation tools, tactics, procedures, and the associated artifacts.

Targeted and precise, HIRT's thorough analysis measures the scope of the incident and the

potential risks to the integrity, confidentiality, and availability of systems that need immediate attention.

Broad Incident Response for State, Local Election Infrastructure

HIRT offers four types of constituent engagement for incident response:

- Remote assistance,
- Advisory deployment,
- Remote deployment, and
- On-site deployment.

HIRT incident response is action taken to respond to the suspected incident and address the increased risk resulting from the incident. The goal is to manage the situation in a way that ensures safety, limits damage, and reduces recovery time, costs, and risk.

In addition to incident-specific hunt analysis, incident response services include:

- **Incident triage**: Process taken to scope the severity of an incident and determine required resources for action
- **Network topology review**: Assessment of network entry, exit, remote access, segmentation, and interconnectivity, with subsequent recommendation to enhance security
- **Infrastructure configuration review**: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)
- **Malware analysis**: Reverse engineering of malware artifacts to determine functionality and discover indicators
- **Mitigation**: Actionable guidance to improve the organization's security posture, including incident-specific recommendation, security best practices, and recommended tactical measures

Following completion of the incident analysis, HIRT will deliver an Engagement Report typically within 30 days to 60 days. The report provides background, scope, findings, security best practices, and conclusions relevant to the hunt.

HIRT encourages reports of cybersecurity incidents, possible malicious code, vulnerabilities, and phishing attacks. Submit a report via phone: 1-888-282-0870 or email: NCCICCustomerService@hq.dhs.gov. For more information, visit www.dhs.gov/cyber.

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