



EIS Communiqué

Sharing Election Infrastructure News and Resources

March 21, 2018

Volume 1, Issue 8

Election Infrastructure ISAC Stood Up

Cyber threat intelligence, network monitoring, incident response and remediation, and more are essential elements for robust cybersecurity and are now available through a new watch and warning center tailored to and for the election infrastructure community.

The Election Infrastructure Subsector Government Coordinating Council (EIS GCC) voted at its February 15 meeting to turn a four-month pilot into an ongoing operational reality for the country's election infrastructure. The EIS GCC is a 27-member group of 24 state and local election officials and three federal government officials working in a whole-of-government approach to secure the Nation's election infrastructure.

The new Department of Homeland Security-backed center coordinates and shares information on election security. Announced on March 7, the Elections Infrastructure Sharing and Analysis Center (EI-ISAC) gives state and local jurisdictions a dedicated venue to share information about cyber threats and vulnerabilities specific to elections systems.

The EI ISAC serves the election infrastructure community through:

- 24 x 7 x 365 network monitoring
- Election-specific threat intelligence
- Threat and vulnerability monitoring
- Incident response and remediation
- Training sessions and webinars
- Promotion of security best practices

The 120-day pilot ran from Oct. 12, 2017 through Feb. 9, 2018. Election officials in seven states and two counties participated in the pilot: Colorado; Indiana; New Jersey; Texas; Utah; Virginia; and Washington; and Travis County, Texas and Weber County, Utah.

Objectives of the pilot included:

- Understanding the MS-ISAC role, mission, and services available to members;
- Working together on product development to share insightful information and warnings on cyber security threats to Election Infrastructure;



Homeland Security

- Helping state and local election stakeholders better understand the cyber threats to their infrastructure;
- Creating a community of interest on the Homeland Security Information Network (HSIN) to provide a workspace for collaboration and centralized access to all shared products.
- Working jointly to deploy the Albert sensors to monitor election infrastructure networks.
- Developing and testing of a notification process should a cybersecurity incident occur.

The pilot showed that an ISAC tailored to the elections community significantly improves communication with and among the elections community as well as enhances cyber defense tools and capabilities that serve to protect elections infrastructure.

Membership in the EI-ISAC is open to all state, local, tribal, and territorial (SLTT) government organizations and associations that support elections in the United States. DHS encourages state and local elections agencies to take advantage of this initiative to harden the cybersecurity posture of the elections sector. **To join the EI-ISAC, please complete the [registration form](#).**

The MS-ISAC mission is to improve the overall cybersecurity posture of the Nation's state, local, tribal, and territorial (SLTT) governments through focused cyber threat prevention, protection, response, and recovery. Operational in 2003, the MS-ISAC works closely with the DHS National Protection and Programs Directorate's own 24 x 7 watch and warning center, the National Cybersecurity and Communications Integration Center, or NCCIC.

MS-ISAC membership is open to all U.S. SLTT government entities at no cost. Membership in the EI-ISAC also provides access to all MS-ISAC products and services.

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.



Homeland Security

Purpose

The EIS Communiqué series will periodically inform subscribers of the myriad 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](#)