IT-ISAC
Elections Industry – Special Interest Group
Participation in the IT-ISAC

- The Information Technology Information Sharing and Analysis Center was founded in 2000 and became operational in 2001.

- Not for profit corporation owned by the members and managed by the Board of Directors.

- Global membership from a diverse set of companies that produce, use, and leverage IT products and services.

**IT-ISAC Mission:**

- Grow a diverse community of companies that leverage information technology and have in common a commitment to cybersecurity.

- Serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.
Information Sharing Relationships

IT-ISAC

National Council of ISACs
(24 Member ISACs)

- NCC COMM-ISAC
  - 65 Industry Members
  - 6,000+ Members

- REN-ISAC
  - 500+ Members

- E-ISAC
  - 6,000+ Members

- FS-ISAC
  - 8+ Federal Agencies
  - 6,000+ Members

- EI-ISAC
  - 1,100+ Members

- MS-ISAC

International Partners

Open-Source Reporting

Partner-intelligence Reporting

ICCT-ISAC Japan

FIRST

DHS

Automated Connection

Customers of Members
(1,000,000+)

Global Membership
Elections Industry-Special Interest Group

• The IT-ISAC EI-SIG was formed in August 2018 with the following goals:
  • Provide a forum for trusted information sharing and collaborative analysis among IT-ISAC members who operate within the elections industry;
  • Better enable members to increase their abilities to identify threats to, vulnerabilities in, and mitigate attacks on their corporate enterprises and/or their products.

• The EI-SIG proactively demonstrates industry’s commitment to election security and serves as a trusted forum for members to share effective risk mitigation practices.

• It promotes to DHS and SLTT governments an organized, consensus-based industry perspective on operational and security matters.
Coordinated Vulnerability Disclosure

- Voting vendors face challenges unique to the elections industry.

- The EI-SIG has identified the need for an industry-specific coordinated vulnerability disclosure program.

- With a proper CVDP in place, voting vendors will have a clear and direct process to take in order to ensure their voting machines are secure and free of potential vulnerabilities.

- Through identifying this need, the EI-SIG produced a white paper on their commitment to develop a CVDP and followed up by releasing an RFI requesting input from the public on how to properly execute the program.
What’s Next

• Our Goal: Ensure election security and voter confidence by implementing a successful coordinated vulnerability disclosure program, suitable to the elections industry, where a variety of trusted researchers are given the opportunity to discover vulnerabilities in voting machines, disclose the information to vendors, and work together in fixing vulnerabilities in a timely manner.

• The EI-SIG is reviewing RFI feedback and engaging across the elections community to create a coordinated vulnerability disclosure program that has the support of a broad range of stakeholders.
EI-SIG Members

- BAE Systems
- Clear Ballot
- Dominion Voting Systems
- Election Systems & Software
- Hart InterCivic
- Smartmatic
- Unisyn Voting Solutions