Elections Industry-Special Interest Group: Frequently Asked Questions

Q: What is the IT-ISAC?

The Information Technology-Information Sharing and Analysis Center (IT-ISAC) is a non-profit, limited liability corporation formed by members within the Information Technology sector as a unique and specialized forum for managing risks and corporations' IT infrastructure. Members participate in national and homeland security efforts to strengthen the IT infrastructure through cyber information sharing and analysis. As a result, members help their companies improve their incident response through trusted collaboration, analysis, coordination, and drive decision-making by policy makers on cybersecurity, incident response, and information sharing issues. The IT-ISAC is multi-faceted, meaning that it supports not only core IT providers and manufacturers, but also those that leverage IT for critical business functions. Our two core functions are to provide companies **intelligence** they need to manage risks to their respective enterprise (protecting the ".com" space) and industry specific **communities** where businesses can engage with each other on common technology-related concerns.

Q: What is the IT-ISAC Elections Industry-Special Interest Group (EI-SIG)?

With a mission to collaborate information and improve the safety of our voting systems, the EI-SCC (Election Infrastructure Sector Coordinating Council) and the IT-ISAC formed a Special Interest Group (SIG) for companies in the Elections Infrastructure Subsector. The Elections Industry Special Interest Group (EI-SIG) provides a dedicated forum for companies with common lines of business to proactively facilitate and support the sharing of threats (cyber and physical) in a trusted environment and to explore solutions driven by industry needs. In contrast with the government focused EI-ISAC, this group is led by corporate members, who participate with the same benefits available to other IT-ISAC members. Election companies who are a part of the SIG have valuable peer access to major IT and cybersecurity companies, which helps elevate the cybersecurity posture of their respective companies, and the Elections Subsector as a whole.

Q: What is the cost to join the EI-SIG?

The IT-ISAC provides EI-SIG members with access to a Threat Intelligence Platform (TIP), develops analytical reports for staying on top of developing threats and industry trends, and provides staff to support elections industry member engagement. To carry out this work, the IT-ISAC has a tiered dues structure, with Bronze Membership ($3,000), Silver Membership ($8,000) and Gold Membership ($25,000). Applicants can choose their own membership level. A chart detailing specific benefits at each level is provided on the next page.

BENEFITS OF IT-ISAC MEMBERSHIP (List of Services)	FOUNDATION Gold ($25,000)	PREMIUM Silver ($8,000)	PARTICIPANT Bronze ($3,000)
Guaranteed Board Memberships	2	0	0
TruSTAR Credentials	20	10	7
Number of persons receiving daily IT-ISAC Report	15	5	5
Number of persons with access to the IT-ISAC Technical Committee weekly meeting	10	5	2
Number of IT-ISAC Special Interest Groups your company can participate in	Unlimited	3	1
STIX/TAXII Integration	✔	✔	✔
Premium API Access	✔	✔	
Website + Brochure	✔		
Discount on Additional TruSTAR Services	✔	✔	✔

Q: How does the IT-ISAC share information with DHS?

The IT-ISAC shares information with DHS or other government agencies only when the sharing company has given the IT-ISAC the explicit permission to do so. It also has access to indicators from DHS through the DHS Automated Indicator Sharing Program, and the Cyber Information Sharing and Collaboration Program. Further, the IT-ISAC also collaborates with the MS-ISAC and other established ISACs through the National Council of ISACs.

Q: How do I join the Elections Industry-SIG?

Companies in the elections industry who are interested in joining the SIG should contact Scott Algeier the IT-ISAC Executive Director at salgeier@it-isac.org for an application to join the IT-ISAC.

Value to Elections Industry Community

Daily Reporting:

IT-ISAC Members have the benefit of receiving daily reporting on trending cyber news, threats, whitepapers, vulnerabilities, patches and exploits. The IT-ISAC team monitors numerous outlets and platforms every day, so members can consume the information while focusing on their own organizational risks. Among our information sources are reporting from our National Council of ISACs partners, DHS CISCP/AIS reports, trending CVEs, malware and IOCs via our Threat Intelligence Platform (TIP) provider, [TruSTAR Technologies](#). Our threat reports provide links that take you directly into the TIP, allowing for analytical review. The IT-ISAC also creates "Breaking News Reports" periodically for certain topics such as, Petya/NotPetya, WannaCry, Equifax, BadRabbit, etc. These reports consist of compiled open-source news, member reported information, partner reported information and any related IOCs in the platform. All IT-ISAC members receive access to the TIP and to all of our reports.

Technical Committee/IT-ISAC Member Base:

The IT-ISAC Technical Committee gives members the ability to engage directly with analysts from other IT-ISAC members. Members communicate with each other via chat, listserv or on weekly calls. This easy, direct contact allows provides a great forum for issuing a request for information, sharing information about an attack or incident, or to ask for assistance on a problem you might be experiencing. The Tech Committee also hosts guest speakers from members and non-members to brief on research/whitepapers they have completed, recent attacks or incidents, trends, or other topics of interest. Additionally, this forum is open for members to discuss trending topics, pose questions to the group or simply brainstorming ideas for a project. At each meeting time is reserved for members to bring forth any items of interest they would like to discuss or need assistance with.

Incident Reporting/Active Attacks:

The IT-ISAC actively updates the membership with information regarding severe cyber related incidents, APT actor campaigns, and critical vulnerability threats. Our incident reports feature a plethora of open source news sources, direct manufacturer details, and additional IT-ISAC member supplied commentary from various security experts. These reports typical feature a detailed description of the situation, the incidents potential impact, and mitigation information to ensure members can protect their systems. The IT-ISAC continues to monitor the situation and updates the membership when new details emerge.

Contact our Executive Director, Scott Algeier (salgeier@it-isac.org) for membership inquiries.