Elections Infrastructure ISAC™

2018 Year in Review

EI-ISAC®

2018 Year in Review

CIS® Center for Internet Security®

Table of Contents

Overview

We can achieve more collectively than we can individually.

This guiding principle of the Elections Infrastructure Information Sharing & Analysis Center™ (EI-ISAC®) was evident throughout its inaugural year.

During 2018, the EI-ISAC evolved from an idea to a formalized collective of dedicated election officials, their staff members, associations, technology vendors, federal partners, and cybersecurity experts working tirelessly to help secure the U.S. elections infrastructure. From sharing information about the threat landscape to creating educational opportunities and implementing technical cybersecurity controls, the EI-ISAC's members, staff, and partners made substantial strides toward ensuring the security and integrity of our elections.

The EI-ISAC is a voluntary and collaborative effort based on a strong partnership between CIS® (Center for Internet Security®), the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC).

This initiative dates back to January 2017, when DHS designated election infrastructure as a critical infrastructure subsector. Following this designation, the EIS-GCC was established consisting of representatives from DHS, the U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED).

The newly formed EIS-GCC determined that an Information Sharing and Analysis Center (ISAC) focused on election infrastructure would provide immense value to the elections community and recommended its creation. The next step was implementing a pilot program to test the viability of the idea and to develop a framework that would prove the value of the new ISAC and establish a clear path forward. The EIS-GCC turned to CIS and MS-ISAC® (the Multi-State Information Sharing & Analysis Center®) to support these efforts, as the MS-ISAC had been designated as DHS's key cybersecurity resource for cyber threat prevention, protection, response, and recovery for all U.S. State, Local, Tribal, and Territorial (SLTT) governments. After the completion of the pilot, which ran from October 2017 until February 2018, the EIS-GCC held a vote on February 15 to formally launch the Elections Infrastructure ISAC on March 7, 2018.

The EI-ISAC has continued to evolve since its creation, and offers its members a variety of services that include the following:

- Access to a 24/7/365 Security Operations Center (SOC)
- Cyber incident response and remediation
- Threat and vulnerability monitoring
- Election-specific threat intelligence
- Training sessions and webinars
- A National Cyber Situational Awareness Room (NCSAR)
- Security best practice recommendations and tools

The EI-ISAC has positioned itself at the forefront of our nation's effort to secure our election systems, and will continue to operate in partnership with members and stakeholders nationwide to ensure the integrity of elections in the United States.

The Pilot

The EIS-GCC and MS-ISAC first began their formal collaboration in October 2017 with a pilot that included representatives from seven states (Colorado, Indiana, New Jersey, Texas, Utah, Virginia, Washington) and two local election organizations (Travis County, Texas; Weber County, Utah). The DHS Election Task Force (ETF), EAC, and NASED worked alongside the MS-ISAC to develop a program that could serve as an ISAC for the Election Infrastructure Subsector. The MS-ISAC quickly formed an elections team to leverage their existing suite of products and services, as well as their relationships with state and local government IT staff, to address the vision of the pilot participants.

Throughout the subsequent five months, pilot participants offered insight and expertise through weekly calls and open lines of communication that would lead to the creation of an Elections-Focused Cyber Defense Suite. The development of elections-focused products and services presented challenges for the MS-ISAC's newly formed elections team, who were accustomed to working with Chief Information Security Officers (CISOs), Information Technology (IT) staff, and other Information Security constituents. Providing valuable resources for the elections community meant pivoting from the more strictly technical content of the MS-ISAC and offering executive level context and guidance specifically for election officials.

The pilot helped focus these efforts, which resulted in the creation of four new product lines that leveraged a new set of subject matter experts and created a robust formal notification process for its new stakeholders.

Beyond adapting their approach, the EI-ISAC was presented with logistical challenges as well. The pilot program called for the deployment of "Albert," the MS-ISAC's Intrusion Detection System (IDS), on every pilot state's elections network to protect the voter registration database if it was not covered by an existing Albert sensor. This required securing the funding and approval, deciphering whether each state was covered, working with the states to execute agreements, identifying and educating stakeholders from various departments and vendors, ordering and configuring the hardware, and, finally, supporting the pilot members during installation. This effort had election officials and information security leaders successfully working hand-in-hand to help the EI-ISAC staff navigate the logistics of this challenge.

Even with the enormous dedication of the pilot participants, Albert deployments proved to be a challenge, with only five of the seven states successfully incorporating Albert sensors by the end of the pilot phase. The remaining two states were not far behind – one state went online the day after the pilot closed, and the final pilot sensor was installed and running by early March.

On February 15 the EIS-GCC reviewed the pilot's current efforts and future plans, and voted in favor of the formal creation of the EI-ISAC, operated by CIS alongside the MS-ISAC. The following weeks were filled with collaboration across CIS to create the permanent infrastructure necessary to formalize the EI-ISAC's efforts. This infrastructure included legal agreements, a webpage and a way for members to join, staff training, and further collaboration with the partners and leadership that had supported them thus far. The Elections Infrastructure Information Sharing & Analysis Center was formally launched on March 7, 2018.

MS-ISAC Integration

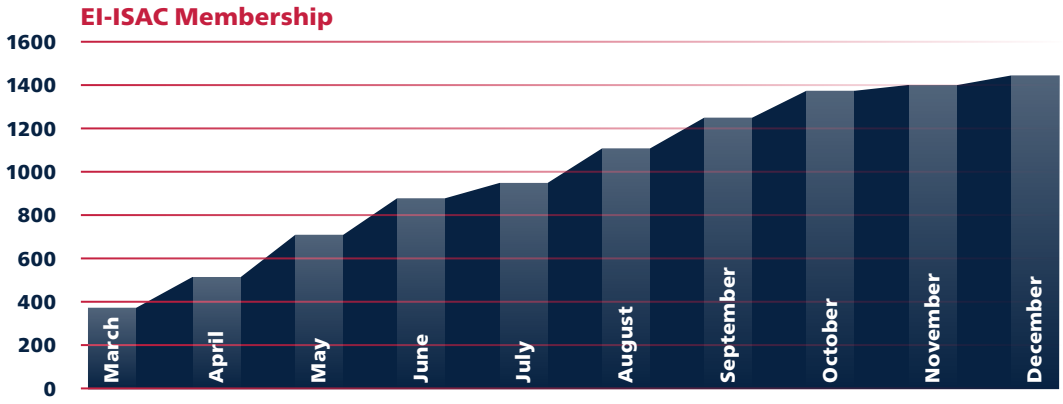
The EI-ISAC was conceived as a means of leveraging the many capabilities and the infrastructure of the MS-ISAC. The integration of the two continued after the EI-ISAC's formal launch in March. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices of CIS. This allows them to work together to educate and protect SLTT governments from the myriad cyber threats that are aimed at both the traditional government IT systems and those specific to elections.

Both ISACs continue to utilize centralized, and in many cases shared, resources to enable a greater level of visibility and information sharing across the elections and the SLTT government sector to benefit the constituencies of both organizations. Furthermore, everything from webcasts to workgroups to in-person meetings integrate the needs of both ISACs, offering efficiency and consistency for the Membership. The support structure behind the ISACs includes:

- Security Operations Center (SOC) to provide 24/7/365 incident triage and immediate response.
- Computer Emergency Response Team (CERT) to provide incident response and forensic services.
- Cyber Intelligence Team to provide forward-leaning analysis, written products, and presentations.
- Engineering Team to provide sensor deployment and technical assistance.
- Stakeholder Engagement Team to provide member support and engagement.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Promoting Engagement



Membership

When the EI-ISAC was formally launched, the supporting partners—including the NASS, NASED, Election Center, EAC, and International Association of Government Officials (iGO)—graciously assisted the EI-ISAC in spreading the word of the new structure. An informational kickoff webcast was held on March 16, and by the end of the month the EI-ISAC had 364 member organizations. This growth continued throughout 2018, and by the end of the year, the EI-ISAC boasted 1,447 members in total, making it the fastest-growing ISAC of any critical infrastructure subsector. Members include all 50 states, three territories, 1,384 local governments spread across 44 states, seven associations, and 14 supporting members from the private sector. This included seven states (Florida, Maryland, Nevada, New York, Ohio, Rhode Island, and South Carolina) with 100 percent participation by the state's local elections offices.

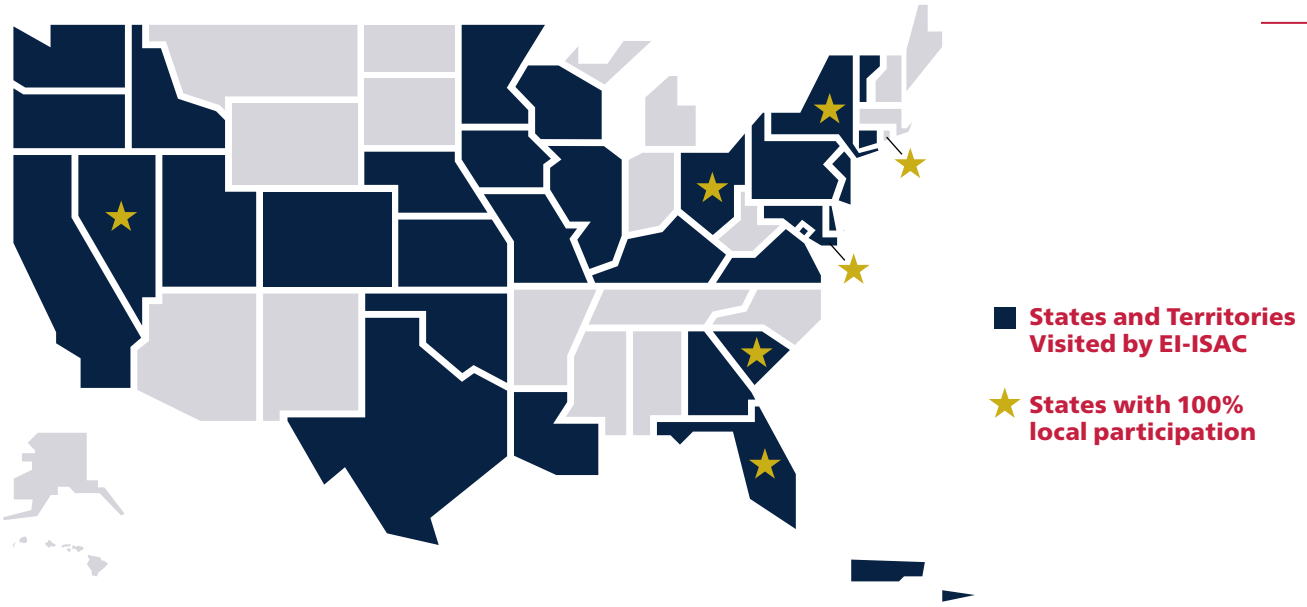
While integration with the existing MS-ISAC foundation was paramount for the EI-ISAC's success, the added pressure of an upcoming midterm election sparked staff across CIS and both ISACs to continuously analyze the efficiency of their processes. This spirit was evident even on the day the ISAC was launched.

Traditionally, while membership in the ISACs has always been no-cost, members were required to complete a Membership Agreement in order to join. While this document was not extensive, it did create an extra step in the process. To streamline the membership process due to the large number of elections offices that were joining, ISAC staff worked with teams across CIS to make one seemingly small change: replacing the Membership Agreement (which required handwritten signatures of both parties) with a checkbox on the online registration form for potential members to agree to a set of terms and conditions. This led to unprecedented membership growth in both the EI-ISAC and MS-ISAC; in fact, MS-ISAC membership grew by over 150 percent in 2018.

Events

While simplifying the process to join was instrumental, the EI-ISAC also needed to reach out to potential members and inform them that these resources existed. EI-ISAC staff attended more than 40 events across 29 states and three territories in 2018 to spread awareness about the new organization and the services available to state and local elections offices. In addition to the efforts of EI-ISAC staff, partner organizations and members banded together to inform potential members about this new organization and to encourage them to join.

While spreading awareness and growing the membership of the EI-ISAC were key initiatives, these events also focused heavily on preparing election officials for the primary and general elections and on providing cybersecurity education. For instance, in New York, Colorado, and Illinois, EI-ISAC staff participated with election officials in tabletop exercises created to give



participants the opportunity to practice handling cybersecurity scenarios that could occur during an election. In Washington and Kansas, EI-ISAC staff participated in cyber-focused trainings to broaden election officials' knowledge base.

In addition to traveling across the nation to support member and partner initiatives, the EI-ISAC also hosted its own webcasts throughout 2018. This included informational sessions for new and prospective members and a joint Monthly Member Call with the MS-ISAC to provide updates, best practices, and a look at the current threat landscape. In October, the EI-ISAC hosted its first Quarterly Membership Call, attended by more than 250 members, which highlighted observed activity and cybersecurity posture in advance of the upcoming November 6 Election Day.

In April 2018, the EI-ISAC joined forces with the MS-ISAC for its Annual Meeting in New Orleans. EI-ISAC members used the meeting as an opportunity to network, learn from one another and the ISAC staff, and discuss cybersecurity with subject matter experts from across the country. During the course of this three-day event, the EI-ISAC held special elections-focused sessions where more than 30 members were able to share perspectives on challenges, best practices, and considerations for elections security.

The newly formed EI-ISAC used this special elections-focused session to learn what the top concerns were for its members and partners in order to better prioritize the services being developed. The Membership stressed that creating uniform messaging to the public was, as always, a major topic of concern. Other critical concerns were the need to define what election infrastructure includes, determining the role the EI-ISAC would play in security, and suggestions on ways that states could provide assistance to local elections offices. This was one of the first times the EI-ISAC acted as an instrument for true peer-to-peer information sharing, with discussions covering one state's plan to create a "cyber navigator" program, plans for integration with fusion centers, sharing insight regarding federal resources available to elections offices, and the sharing of useful guides and templates between members.

Partnerships

The EI-ISAC could not have achieved the success that it has without the expertise and camaraderie of many organizations in government and industry. From the expertise of NASS and NASED at the state level, to iGO and the Election Center's valuable insight into local government election organizations, the EI-ISAC has been fortunate to have the strong support of the elections community. The invaluable support and guidance of DHS made it possible for EI-ISAC services to be available at no-cost to all members, while simultaneously supporting the purchase and deployment of IDS sensors for elections offices around the country. The EIS-GCC and the pilot participants provided much-needed direction and support to the young EI-ISAC, and the EIS Sector Coordinating Council (EIS-SCC) offered important insight into the crucial partnerships between vendors and elections offices, allowing the EI-ISAC to understand what it would take to truly support its Membership.

In addition, working with the FBI's Cyberhood Watch provided the EI-ISAC with an opportunity for bi-directional sharing of valuable threat information, while other partners like Democracy Works furnished information to assist with outreach to local elections offices. Creating and fostering these partnerships accelerated the acceptance of the EI-ISAC as a trusted resource for its Membership, an essential quality for its mission to improve the overall cybersecurity posture of U.S. elections offices.

Addressing the Threat

The Elections-Focused Cyber Defense Suite created by the EI-ISAC offers members a variety of resources and services to help secure their organizations and information, ranging from a federally funded Intrusion Detection System (IDS) with 24/7/365 support, almost 100 intelligence products, and a National Cyber Situational Awareness Room for coordination and collaboration on election days.

Albert

A focus of the EI-ISAC's efforts throughout 2018 was a federally funded initiative to deploy its IDS, known as Albert, on elections networks throughout the United States. Under the MS-ISAC, sensors had already been funded for each state and territorial network and were developed to be specific to the SLTT government environment. The EI-ISAC expanded this initiative to cover the voter registration databases of any state or territory where the voter registration database was not already covered by an existing sensor, as well as to place sensors in 42 of the most populous local election jurisdictions in which voter registration data were hosted on local hardware.

The Albert expansion benefited the entire EI-ISAC community by providing a deeper understanding of, and actionable intelligence on, the threats directly affecting the elections community. This knowledge informed EI-ISAC members so that they could create tailored response plans to shifts in the cyber threat landscape, while simultaneously allowing both DHS and the EI-ISAC to focus future services to the needs of the Membership. After identifying two pilot states as being covered by existing sensors and successfully implementing sensors on the remaining five pilot states, the EI-ISAC identified an additional 18 states covered by existing sensors.

> *"The Albert sensor was a great benefit to our small agency. We use many of your services and we recommend them to our counties, and we are in deep gratitude for your mission and the professionalism in which you carry it out. You are truly making a difference to the security of elections in our state and across the nation."* – EI-ISAC Member

The EI-ISAC launch in early March gave the team eight months to deploy as many of the remaining 72 federally funded Albert sensors as possible prior to the general election.

Since ordering and receiving a sensor typically takes three to five weeks, the EI-ISAC team expedited the process by ordering sensors in blocks of 15 to 20 based on the sizing information obtained during the ISAC pilot and supplemental incoming data from the states. Additionally, the EI-ISAC developed a survey that allowed the sensors to ship immediately to each organization once complete. This streamlined the process, building in faster procedures along with concurrent actions, which negated the need to wait for the completion of a Pre-Installation Questionnaire before shipping the hardware.

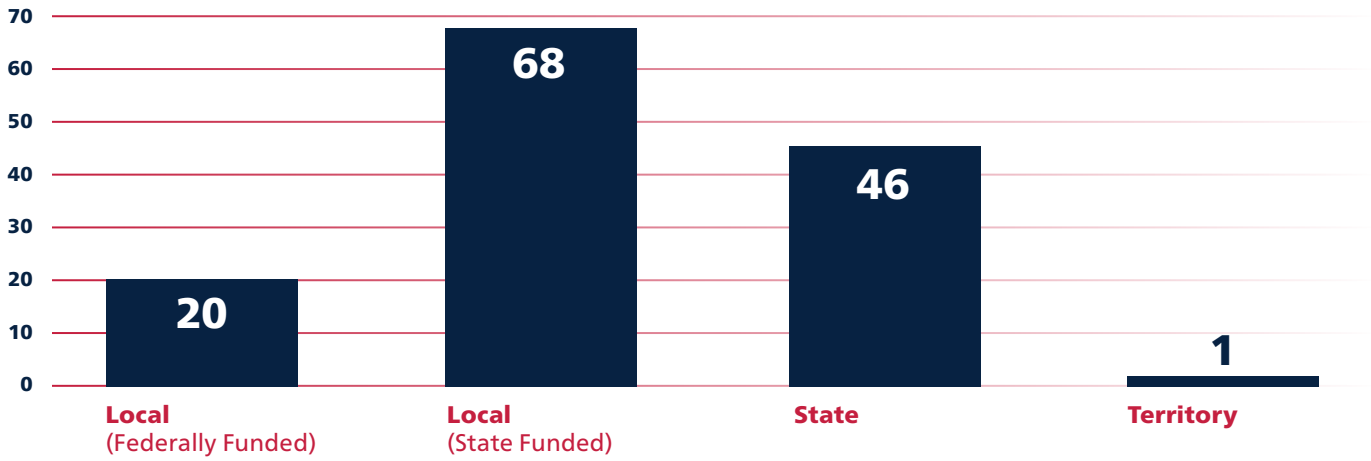
A combination of logistical expediting, a Membership that was incredibly supportive of the efforts, and extensive outreach and technical support efforts by EI-ISAC staff and partners paid off with DHS Secretary Kirstjen Nielsen sharing that on Election Day, approximately 90 percent of all voters in the United States would cast a ballot in a jurisdiction or state monitored by Albert.

Once Election Day 2018 arrived, 45 states, one territory, and 84 local jurisdictions (18 of which were federally funded) had Albert sensors protecting their voter registration data. This was a monumental feat considering that many of the eligible organizations had never heard of Albert or the EI-ISAC nine months earlier.

The teamwork shown by the combined ISAC staff, elections offices, and information security staff that support them—and the fact they created the Albert network that has now been deployed across the country—demonstrates that our partners feel the same way, and the numbers speak for themselves. As of the end of 2018, the elections-specific Albert devices had reported 155 billion records and a total of 10 petabytes of data, leading to 3,389 actionable notifications to members.

Having a couple of Albert sensors here and there does not provide a big picture or additional situational awareness. However, when these sensors are deployed nationwide, experts at the ISAC are able to track trends and intrusions and then share that information with election organizations at both the state and local level to better prepare them for the challenges that lie ahead. According to CIS President and CEO John Gilligan, "When you start to get dozens, hundreds of sensors, like we have now, you get real value."

Albert Deployments
as of December 31, 2018



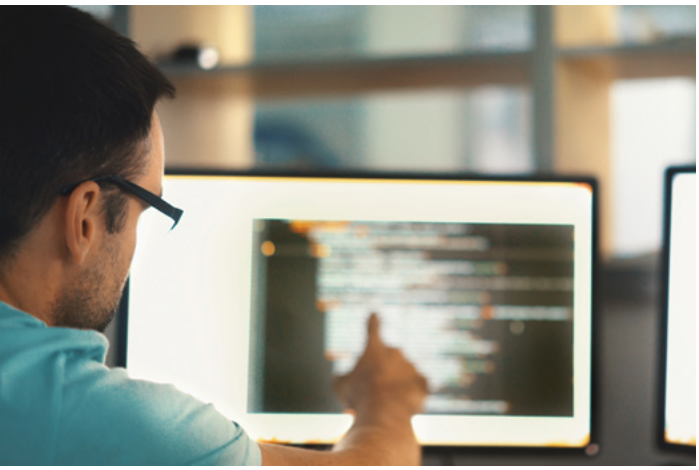
EI-ISAC 2018 Intel Products Disseminated

Products

Through Albert monitoring and incident response and reporting, the ISAC Cyber Intelligence Team was able to identify major trends and changing tactics, techniques, and procedures (TTPs) that affected election organizations. These trends and TTPs included common malware, misinformation efforts, web attacks, suspicious network activity, and malicious emails.

In order to keep the Membership apprised of the changes in the current threat landscape and inform them of mitigation recommendations, the ISAC Cyber Intelligence Team disseminated a variety of elections-specific intelligence and educational products throughout 2018. The Weekly News Alerts provided a summary of recent news articles about cybersecurity, best practices, election industry and legislative action along with analytical context, while the Cybersecurity Spotlights offered EI-ISAC members a non-technical introduction to key cybersecurity terms and how they relate to elections offices and activities. Additional disseminations that offered summary views on the elections-related threat landscape included the Quarterly Threat Reports, Cybersecurity Advisory Summaries, and Intel Bytes, while the very timely Cyber Alerts provided insight into rapidly developing trends and TTPs. During 2018 the EI-ISAC released 92 intelligence and educational products in total.

Other products created by the EI-ISAC offered members a way to more easily leverage existing tools. For example, the resource titled "3 Steps to Secure Your Elections Infrastructure Today" helps election organizations improve their cybersecurity readiness by offering a few key steps to take and how to do so. The "Election Security Services" checklist highlights key services recommended in *A Handbook for Elections Infrastructure Security* (the Elections Handbook) issued by CIS. To help narrow the search for security implementation tools, this checklist highlights key services recommended in the Elections Handbook and the available opportunities to implement them. Pairing the Elections Handbook and checklist with the Election Infrastructure Assessment Tool (EIAT), also developed by CIS in 2018, helps elections offices increase their understanding of the best practices, including the CIS® Controls, they should implement to secure each unique environment.



Sharing Information

Throughout 2018, the EI-ISAC hosted the National Cyber Situational Awareness Room (NCSAR) on 17 separate primary election days, offering EI-ISAC members and designated partners the opportunity to collaborate, share information, and provide observations in real time. The virtual collaboration room relied on the secure HSIN Adobe Connect environment hosted by DHS. Access was restricted to EI-ISAC members in the jurisdictions holding elections, in addition to federal employees and EI-ISAC staff, resulting in a secured environment for the safe discussion of incidents. During this time, incidents reported through the NCSAR included technical difficulties, polling misinformation, and suspicious emails.

Additional Services

The Elections-Focused Cyber Defense Suite adopted a wide variety of other MS-ISAC resources that would be beneficial for elections offices. This included the following:

- The Malicious Code Analysis Platform (MCAP) through which EI-ISAC members submitted and analyzed suspicious files and URLs, and, upon request, received analysis assistance from a member of the EI-ISAC CERT.
- The Malware Submissions inbox through which EI-ISAC members reported suspicious emails for CERT review and analysis.
- The EI-ISAC CERT provided no-cost incident response and digital forensic services to election organizations in five states, offering them someone to turn to when protection measures failed.
- Nearly half of the EI-ISAC Membership provided the SOC with their public-facing IP address. ranges and domains for passive monitoring and monthly vulnerability notifications by the Vulnerability Management Program.
- Using the HSIN platform as a foundation, the EI-ISAC stood up an online portal specifically for the Election Infrastructure Subsector, seeding it with a library of all EI-ISAC published documents as well as discussion boards for members to collaborate.
- EI-ISAC members also received access to an elections-focused area of the Anomali platform, where malicious IP address and domain notifications were stored, as well as Threat Stream, the Anomali indicator research platform.

General Election

Pre-Election Ramp-Up

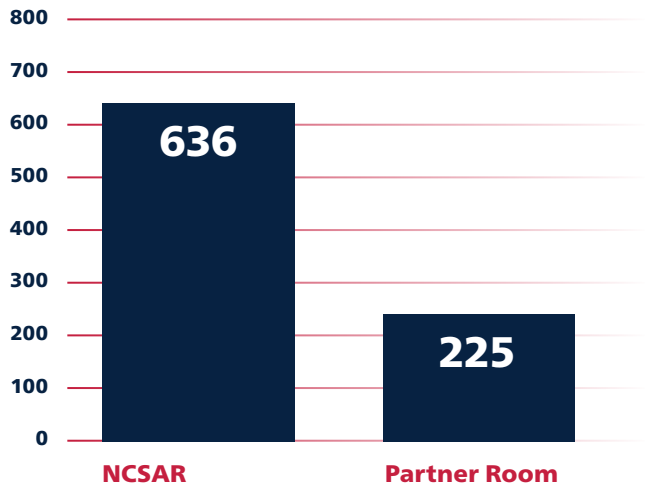
In late September 2018, the six-month-old EI-ISAC went into a heightened response state in preparation for the U.S. general election. This mirrored the elevated posture of the National Cybersecurity and Communications Integration Center (NCCIC), and set the stage for the EI-ISAC to prove its ability to achieve something the election infrastructure community had repeatedly identified as a key goal: *Effective collaboration and communication across agencies and organizations on Election Day.*

To achieve this, the EI-ISAC and DHS executed a community-wide communication plan so that appropriate parties would be notified about incidents and trends; federal agencies and partner organizations would be able to efficiently and securely exchange information; and state and local elections offices would have timely reporting streams and mechanisms. Using a multi-pronged approach to achieve these goals, the EI-ISAC and DHS embedded a DHS Intelligence & Analysis representative at the EI-ISAC headquarters for more than a month prior to the election, heightened reporting through fusion centers to improve accuracy, and developed new, internal reporting streams for information-sharing. At the end of October, an elections-focused Intelligence Analyst from the EI-ISAC was detailed at NCCIC in Washington, D.C., to assist with federal communication with EI-ISAC headquarters.

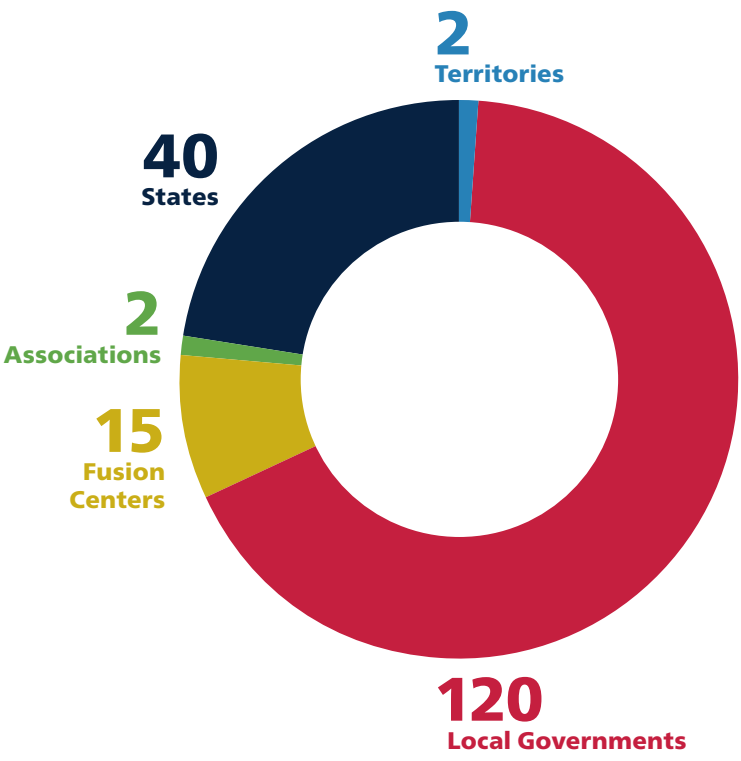
National Cyber Situational Awareness Room (NCSAR)

The NCSAR HSIN room was opened to EI-ISAC members and partners on October 31 for 12 hours each day and transitioned to a 24-hour resource on November 4 for the duration of the week of the general election. Over the two-week span, and especially on November 6, representatives from 40 states, two territories, 120 local government elections offices across 30 states, 15 federally recognized fusion centers, NASS, NASED,vetted vendors of election infrastructure, the Information Technology-ISAC, and the MS-ISAC coordinated activity and shared information. DHS Cybersecurity Advisors, representatives from the ETF, and federal representatives designated by EI-ISAC members also accessed the NCSAR.

Situation Room Attendance



NCSAR Participant Organization Types



General Election
continued

> *"The world of local government cybersecurity is facing increasing new complex threats. The MS-ISAC and EI-ISAC provide much-needed valuable resources. I can honestly say they are on the front lines of our defense with a dedicated team that communicates well with federal and SLTT entities."*
>
> – EI-ISAC Member

In the days leading up to and throughout the general election, 636 participants used the NCSAR to report a variety of common malicious cyber activity, typosquatting, and even non-cyber physical threats. Much of this activity was unsuccessful and indicative of opportunistic and not strategic targeting of election infrastructure.

Election Day

On Election Day, the goal of the EI-ISAC was collaboration: both facilitating it among our members, and also between our members and various representatives at the federal government level. The EI-ISAC increased staffing at its headquarters to provide incident response, NCSAR vetting, support, and assistance to the Membership. Analysts were assigned to myriad special activities, such as writing a Situation Report that was disseminated every four hours, monitoring open source media such as Twitter and other feeds, and maintaining a presence on several other HSIN rooms.

The staffing increases occurred elsewhere too. The elections-focused Intelligence Analyst remained at the NCCIC, joining the ISAC liaison. This facilitated intelligence-sharing with the federal and private sector partners seated at the NCCIC, including DHS I&A and the FBI. Finally, to bring information sharing full circle, two ISAC staff were positioned at the National Fusion Center Association (NFCA), which hosted its own HSIN situation room. There, EI-ISAC representatives were able to get a pulse on what fusion center partners were reporting, offer pertinent information in return, and meet with visitors, including Secretary Nielsen.

On Election Day 2018, an additional HSIN situation room was opened and managed by the ETF. While the EI-ISAC NCSAR remained active, 225 federal employees were kept informed through this additional channel. The EI-ISAC acted as a liaison between the two separate HSIN situation rooms, sharing anonymized data in real time. Real-time sharing of information with EI-ISAC members through the NCSAR and federal situation rooms, with federal partners through the NCCIC, and with fusion centers through the NFCA was important for success. This allowed the EI-ISAC to correlate information between sources, minimize circular reporting, increase the accuracy and speed at which information was disseminated, and have a holistic view of the threat landscape. This approach not only ensured that all points of collaboration were connected but also established a manner for the EI-ISAC to quickly correct erroneous information.

The dedication and collaboration displayed by all the EI-ISAC members and partners was inspiring and something that we should all strive to achieve on every election day going forward.

Looking Forward

Moving into 2019, the EI-ISAC will shift its focus from a period of rapid expansion and growth to expanding the value of activities for its Membership and the elections community as a whole. Formalizing the EI-ISAC mission through the adoption of a charter will be a necessary step toward creating the foundation to achieve these initiatives. This charter will also establish an Executive Committee comprised of EI-ISAC members to lend insight and formal direction for the organization, much in the same way pilot participants steered the initial launch and product suite.

While the EI-ISAC will continue to seek out and participate in opportunities for education, exercise, and achieving its membership goals, such as welcoming the remaining territories and gaining local participation from the six states that that do not currently have local EI-ISAC members, making improvements in technology, and adding new products and services, will also be a focus as the organization matures. These initiatives include:

- Technological improvements for the NCSAR to streamline vetting of members and create breakout areas for particular incidents.
- A vulnerability identification and notification system for production systems, especially voter registration.
- Continuing to foster coordination and expand knowledge and awareness of the EI-ISAC's services and role in elections.
- The creation of a platform allowing members to not only collaborate year-round, but also manage their own customized checklist of cybersecurity plans, linked to resources such as the CIS Election Infrastructure Assessment Tool (EIAT) and Elections Handbook *(A Handbook for Elections Infrastructure Security).*

On October 2, 2018, after looking at the progress made, DHS Secretary Kirstjen Nielsen stated, "First of all, the information-sharing is much stronger than it has ever been before."

The EI-ISAC intends to leverage the incredible momentum from 2018 to continue to enhance election infrastructure security through information sharing, intelligence, and the services and partnerships it creates moving forward.


ELECTIONS INFRASTRUCTURE
ISAC

Elections Infrastructure ISAC™

518.880.0699
elections@cisecurity.org
www.cisecurity.org/ei-isac

CIS® Center for Internet Security®