This document was created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint Subsector-Specific Plan Working Group.

Election Infrastructure Subsector-Specific Plan: 2022 Status Update

In January 2017, the Department of Homeland Security (DHS) established the Election Infrastructure Subsector under the Government Facilities Sector through a critical infrastructure designation for election infrastructure. The designation makes it clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. Government has to offer. [1]

Since its inception, the subsector has established and developed strong partnerships among government stakeholders at the local, state, and federal levels and between the public and private sectors, forming both a Government Coordinating Council (GCC) and a Sector Coordinating Council (SCC). These bodies have provided a focused mechanism for collaboration between state and local election officials, the Cybersecurity and Infrastructure Security Agency (CISA), the Election Assistance Commission (EAC), law enforcement, the intelligence community, and private sector partners to enhance information sharing about risks to the Nation's election systems, identify resources to help mitigate such risks, communicate best practices, address identified vulnerabilities, and enable election officials' and private sector partner's access to threat information.

The Joint Election Infrastructure Subsector-Specific Plan (SSP), initially approved by the GCC and SCC in 2020, provided a framework for industry and government partners to establish shared priorities for security efforts in the face of threats to election infrastructure, while also setting a path for ongoing collaboration and capability development. Since the approval of the joint SSP, the threat environment has evolved, and the subsector has responded with new processes and capabilities. Consequently, the previous SSP is no longer operative. The National Infrastructure Protection Plan (National Plan), which provides a guiding framework for all critical infrastructure sectors and subsectors, is under revision by CISA and its stakeholders with expected completion in mid-2022. A refresh of the Election Infrastructure Subsector-Specific Plan is pending, along with the updated National Plan.

In the meantime, this document provides joint interim guidance for the Election Infrastructure Subsector partnership through the 2022 midterm elections. It focuses on the activities that the GCC and the SCC have identified to address the subsector's current security priorities. These efforts aim to boost collective capabilities for responding to national or large-scale incidents and build resilience across the elections ecosystem through coordinated information sharing and risk mitigation.

---

1 The January 2017 Department of Homeland Security designation defines "election infrastructure" as the following: *"storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."* https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

ELECTION INFRASTRUCTURE SUBSECTOR VISION

A unified government and private sector approach to empower the election stakeholder community to build resilience to election infrastructure threats and risks.

ELECTION INFRASTRUCTURE SUBSECTOR MISSION

To coordinate efforts by state and local election officials, private sector and non-profit partners, and the Federal Government to manage risks and secure election infrastructure against new and evolving threats.

Current Issues

Addressing Physical Security for Election Facilities and Personnel

In the lead up to and the aftermath of the 2020 general election, public officials and private individuals whose jobs involved administering elections or supporting those who administer elections became the subject of threatening communication and conspiracy theories. Election facilities, including government offices and tabulation centers, became the focus of protests or other activity. Private industry facilities were also targeted by protests or others making threats and/or looking to disrupt business operations.

State and local election officials must balance security with access and transparency. Election officials operate on principles of open public access and transparency, which can create challenges for adopting physical security principles and practices to protect workers and employees. Voting sites can be soft targets due to their open access and limited security barriers, and Election Day workers are mostly temporary employees.

CISA currently provides the public and private sectors with access to a diverse array of trainings, exercises, and best practice resources that focus on prevalent physical security attack methods (e.g., active shooter, vehicle ramming, and bombing), along with corresponding protective measures through Physical Security of Voting Locations and Election Facilities guidance that election officials and private sector partners can use to improve their physical security posture. Community-based resources are also available through the DHS Center for Prevention Programs and Partnerships to help prevent individuals from radicalizing to violence.

In July 2021, the U.S. Department of Justice (DOJ) created the Task Force on Threats Against Election Workers to lead the federal law enforcement response to threats to the election community and, where appropriate, to criminally investigate and prosecute such threats. In addition to repeated informal communications and outreach, DOJ leadership and representatives from the Task Force provided numerous presentations to the election community on threat collection, preservation, and reporting including in meetings with National Association of Secretaries of State (NASS), National Association of State Election Directors (NASED), Election Center, and a variety of other stakeholder groups.

CISA's Last Mile effort provides customizable posters that jurisdictions can post in their offices detailing state-specific laws governing threats, harassment, and other relevant activity, as well as contact information for federal, state, and local law enforcement. CISA has also provided resources on doxing prevention to help members of the subsector take steps to protect their personal information before it can be made public. Finally, the EAC created a webpage aggregating information for election officials experiencing threats, including mental health resources for those experiencing threats, harassment, or

other unwelcome communications. There is ongoing work to be done to ensure the safety of both election facilities and members of the subsector themselves, including the formal development of protocols for reporting such hostile activity.

Managing Risks to the Supply Chain

The federal government has prioritized efforts to raise awareness around the risks associated with industry supply chains and related products and/or services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to manufacturing and development practices. Understanding and adopting processes to assure product integrity, security, resilience, and quality are all considerations for Supply Chain Risk Management (SCRM) efforts.

In response to Executive Order 13873, CISA's Information and Communications Technology (ICT) SCRM Task Force worked with industry and government partners to:

- Develop a standardized taxonomy of ICT elements (e.g., hardware, software, and services)
- Perform critical assessments on these ICT elements with appropriate stakeholder input
- Assess the national security risks stemming from vulnerabilities in ICT hardware, software, and services including components enabling 5G communications.

Representatives of the Task Force have met with Election Infrastructure SCC leaders to keep industry partners apprised of their progress.

In June 2021, the Election Infrastructure SCC established a Sector Coordinating Council SCRM Working Group to explore potential practices and risk mitigation efforts within the subsector. The SCRM Working Group seeks to assist election technology providers and election officials with procurement practices around election-related software, hardware, and services to assess and reduce risks to the election jurisdiction and their supply chain partners. In today's global economy, it is almost impossible not to rely on a supply chain that stretches to all parts of the globe. As such, supply chain risk management is necessary to ensure that election officials and their supply chain partners only procure election-related software, hardware, and services from legitimate sources that have a program in place to ensure supply chain integrity.

In February 2022, the SCRM Subgroup on Ballot Paper issued a white paper outlining risk mitigations for subsector partners regarding ballot paper and envelopes. The Working Group also released a document in March 2022 as an introduction on how organizations and downstream supply chain partners, including election officials, can better secure their supply chain. It seeks to provide the following information related to election supply chain risk management:

- Provide SCRM Working Group guidance on election software related supply chain risk management in order to assist others when procuring election related software, hardware, and services;
- Leverage existing resources provided by CISA and the ITC SCRM Task Force;
- Provide checklists and other resources that technology providers and election officials may use to assess their election software supply chain risk management strategy;
- Identify best practices regarding software supply chain risk management within the election community; and

- Share resources through the election community to increase awareness of supply chain risk management practices.

This work compliments efforts by a range of stakeholders to update the federal Voluntary Voting System Guidelines (VVSG[2]), approved by the U.S. Election Assistance Commission (EAC). These guidelines cover design, development and testing specifications for accuracy, security, functionality, privacy, usability and accessibility of certified voting systems. Voting system manufacturers who submit voting system to the EAC for testing and certification currently provide a range of product and component sourcing and supplier information to the federal government.

Securing Chain of Custody

Prolonged public attention on the administration of elections means that the processes by which election officials secure equipment and materials are under a microscope. Referred to as "chain of custody," these processes include how officials ensure the continued integrity of everything from ballots to pollbooks to voting machines during their life cycle, including their control or transfer from place to place or person to person. This may also extend to digital information or records to ensure that integrity and confidentiality are not compromised. While each state and territory have their own jurisdiction-specific requirements, it is critical that election officials also understand the role that chain of custody procedures play in the broader security of the election ecosystem. In addition, most private sector election support providers have contractual agreements outlining permissions for third-party access to equipment.

According to DHS, chain of custody threats can result in unscheduled disruptions (i.e., equipment malfunction), criminal incidents and terrorist attacks, cyber incidents, supply chain attacks (exploiting vulnerabilities to cause system or network failure), or foreign influence operations (to spread misinformation or undermine democratic processes). Specific to elections, the loss of physical or digital control of chain of custody can result in election offices being unable to provide assurance that equipment or records have not been tampered with or manipulated in violation of established processes.

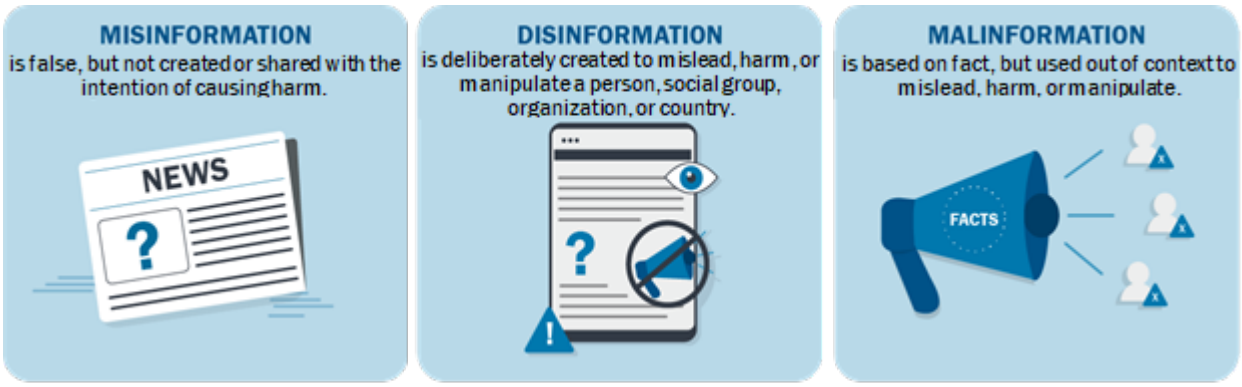
In 2021, both CISA and the EAC issued guidance documents on chain of custody focusing on critical infrastructure generally, and elections. Additionally, a recently developed CISA training, "Building Trust through Secure Practices", addresses implementing and communicating chain of custody procedures. More education and training are needed to help election officials develop and implement chain of custody protocols, including how they pertain to the integrity of the greater subsector.

In addition to educating members of the subsector on chain of custody procedures, state and local election officials must educate their stakeholders—legislators, appropriators, and voters—on these processes to inform decision making and combat mis-, dis-, and malinformation. Further training resources from the GCC on chain of custody can help state and local election officials more effectively communicate on this topic.

[2] Voluntary Voting System Guidelines | U.S. Election Assistance Commission (eac.gov)

Countering Election Mis-, Dis-, and Malinformation

Misinformation, disinformation, and malinformation (MDM) have long posed a threat to election security and integrity.[3] While often inadvertent, misinformation provides voters with inaccurate guidance, such as the incorrect voter registration deadline or voting location, and can be damaging to the point of disenfranchising voters. The malicious forms of MDM are tools used to intentionally confuse voters and undermine confidence in the election process. Taken to their extreme, MDM can result in threats or violence against election workers, officials, or volunteers.



Individual election officials, industry providers, and other organizations represented by subsector councils have implemented efforts to counter MDM. For example, NASS launched the #TrustedInfo initiative to encourage voters to get election information directly from election officials. CISA developed a Rumor Control webpage and many individual states and local election jurisdictions and several election technology providers also produced "rumor control" or "myth vs. fact" webpages to provide accurate information about election administration, technology, and security and to dispel MDM and voter confusion.

After the 2020 election, the GCC and SCC launched the Joint Mis/Disinformation Working Group to leverage opportunities to coordinate efforts across the subsector. Thus far, the working group has created two products to help state and local election officials and industry providers prepare for and respond to risks of MDM: the Rumor Control Page Start-Up Guide and the MDM Planning and Incident Response Guide for Election Officials. The Joint Mis/Disinformation Working Group provides a forum through which the subsector can continue to identify challenges in countering MDM, and it will continue to produce resources for addressing such challenges.

Another approach the subsector has taken to addressing MDM is promoting adoption of the .gov top level domain, available exclusively to U.S. governments. Getting information from a .gov website or email address allows the public to have confidence the information they are viewing is from an official government source. As of April 2021, the .gov program is administered by CISA and is available at no cost. Finally, the information sharing mechanisms discussed below provide information and tools for building awareness of MDM narratives and countering them.

[3] National Intelligence Council, *Foreign Threats to the 2020 US Federal Election*. Intelligence Community Assessment, ICA 2020-00078D, March 10, 2021, https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2192-intelligence-community-assessment-on-foreign-threats-to-the-2020-u-s-federal-elections.

Information Sharing at the Classified and Unclassified Levels

Since its inception, the Subsector Coordinating Council's initial goals and accomplishments focused on the improvement of information sharing. The GCC established the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) to support incident response, trend analysis, and information sharing across the subsector. SCC members belong to the EI-ISAC as supporting members and benefit from the information sharing it provides. An ongoing goal of the GCC and SCC is to increase membership in the EI-ISAC among small to medium-sized election jurisdictions and industry providers. EI-ISAC membership has surpassed 3,000 entities and continues to grow.

The Elections Industry Special Interest Group (EI-SIG) was separately formed by industry technology manufacturers in 2018 through the Information Technology Information-Sharing and Analysis Center (IT-ISAC). The EI-SIG continues to serve as an important vehicle for information-sharing, training, and industry-focused security initiatives, including adoption of organizational coordinated vulnerability disclosure policies.

Subsector members regularly receive threat information from the U.S. intelligence community through ISACs and other avenues, such as classified and unclassified briefings. These briefings from DHS and its federal partners, including the Federal Bureau of Investigation (FBI) and the Office of the Director of National Intelligence (ODNI), allow election officials and industry providers to remain updated on cybersecurity threats and influence operations from foreign adversaries. The subsector continues to add election officials and industry providers to the Election Infrastructure Subsector Clearance Program so they have access to appropriate classified briefings.

Although both the Election Infrastructure Subsector Clearance Program and the EI-ISAC help distribute information, the GCC and SCC continue to advocate for the intelligence community to rapidly downgrade and share actionable intelligence. Unclassified or For Official Use Only briefings and documents can be shared more broadly within the subsector, especially with local election officials, the vast majority of whom do not have security clearance but need access to information to secure their systems and staff. Unclassified briefings also allow the election community to benefit from expertise in the private sector, which can provide a different perspective from the federal government.

The subsector is increasingly looking for ways to share information on physical security threats to election infrastructure, voting locations, and personnel. As the 2022 midterm elections approach, the Subsector Councils acknowledge an ongoing need for improvement related to physical security information sharing, including the development of information sharing protocols.

The GCC continues to encourage use of its voluntary Threat Information Sharing and Incident Reporting Protocols across the subsector. These protocols ensure information is appropriately shared across jurisdictions so that when one jurisdiction is facing a threat, the other jurisdictions can monitor for the same threat. The protocols also guide election officials to incident response resources.

The SCC updated its general guidance incident reporting for member organizations in 2021 and continues to utilize this framework subject to all federal, state, and local requirements for such notifications.

Resources for Enhancing Election Security, including Cybersecurity and Ransomware Attacks

Although the subsector is facing increasing physical security and MDM threats, cybersecurity remains an ongoing priority. The GCC and SCC have a sustained focus on increasing the availability and use of cybersecurity resources, services, and training from CISA, EI-ISAC, and others.

CISA, with the help of the GCC and SCC, encourages election officials and industry providers to continue to utilize their cybersecurity assessments and detection and prevention services including new services that are more scalable to grow their reach across the more than 10,000 election jurisdictions and industry providers. Also, in addition to growing its membership to optimize information sharing, the EI-ISAC is expanding participation in its most recently added services such as Malicious Domain Blocking and Reporting (MDBR).

The GCC Training Working Group recently expanded to include the SCC in an acknowledgement of the importance of training across the entire subsector, not just for election officials. The newly established joint working group advises CISA, EI-ISAC, EAC, and others on areas where training resources are lacking. The phishing and ransomware election-focused trainings, as well as the "building trust through secure practices" courses from CISA are recent additions created based on input from the Training Working Group. Additionally, many state election offices have partnered with the private sector and academia or produced in-house cybersecurity training for employees and local election officials. The EI-SIG offers cybersecurity training to member companies and their employees as well.

The GCC and SCC continue to focus on empowering their members to manage cybersecurity risk and plan for potential incidents. Members of both subsector councils provided input on the Election Security Risk Profile Tool, hosted by EAC and created by CISA, which helps election administration stakeholders assess their risk and prioritize their resources for mitigating risk. CISA's Last Mile effort is a collaborative effort with election officials to produce customized products (e.g., Snapshot Posters, Election Day Emergency Response Guides, and other templates) that address the dynamic or conditional cyber and infrastructure risks of state and local election administrators and industry providers. Many state election offices have worked with their private sector partners and others to produce their own products to enhance preparedness at the state-level, and to help local officials prepare for cyber incident response.