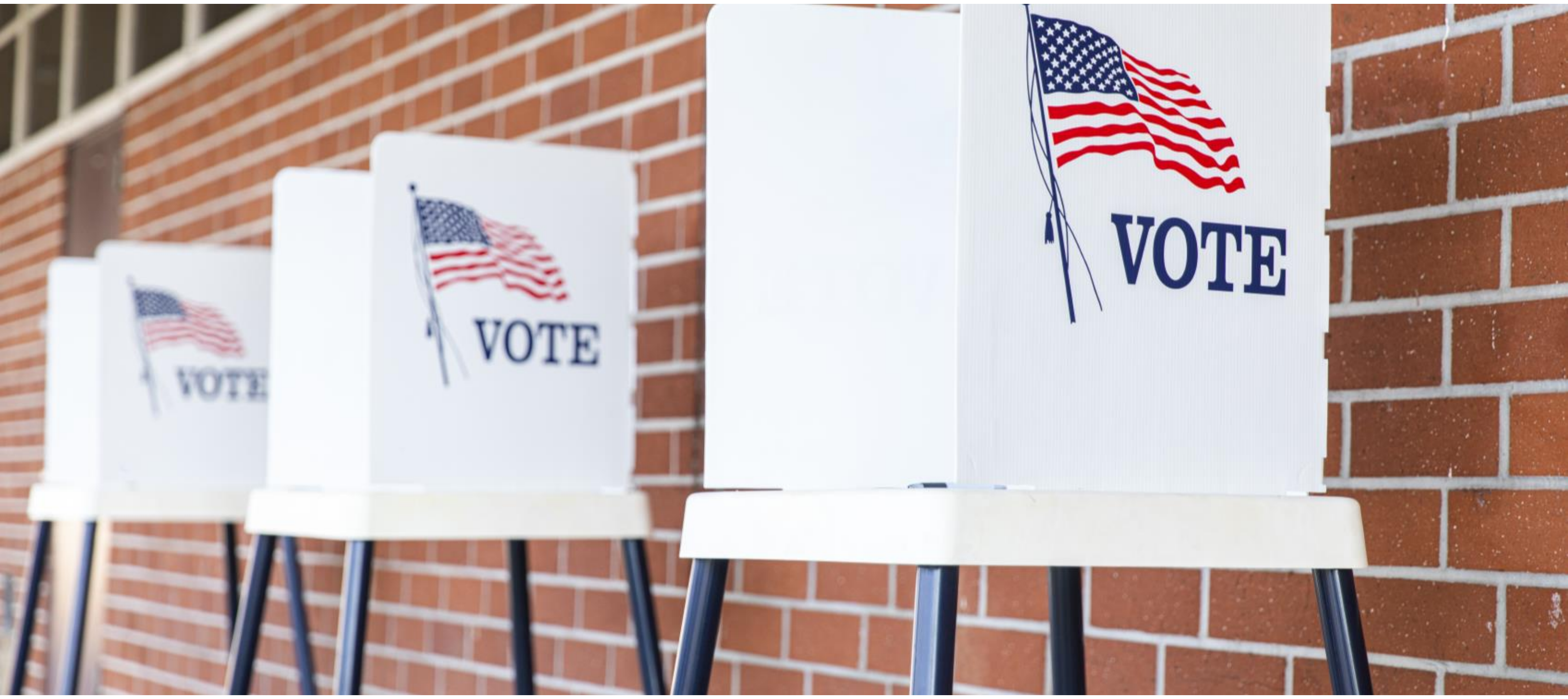

Election Infrastructure Subsector-Specific Plan

2024 Status Update

July 2024

ELECTION INFRASTRUCTURE SUBSECTOR-SPECIFIC PLAN: 2024 STATUS UPDATE

In January 2017, the U.S. Department of Homeland Security (DHS) established the Election Infrastructure Subsector under the Government Facilities Sector through a critical infrastructure designation for securing election infrastructure. Today, the level of coordination between federal, state, and local government and private sector partners is unprecedented. During the years since the critical infrastructure designation, state and local election officials have administered thousands of elections, each one building on the successes and lessons learned from the one before.

KEY ACCOMPLISHMENTS

During the past seven years, the Subsector partners in the public and private sectors have taken significant steps to improve coordination, reduce risk, and strengthen security and resilience capabilities, including:

- The establishment of the Government Coordinating Council (GCC) in 2017 to provide a mechanism for collaboration across federal, state, and local government partners;
- The creation of a Subsector Coordinating Council (SCC) in 2018 to facilitate coordination and information sharing across the private sector;
- The establishment of the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) in February 2018;
- The establishment of the Election Industry Special Interest Group (EI-SIG) under the Information Technology ISAC in 2018.
- The creation and approval of the Joint Election Infrastructure Subsector-Specific Plan (SSP), approved by the GCC and SCC in February 2020, to provide a framework of shared security and resilience priorities for industry and government partners in the face of threats to election infrastructure, while also setting a path for ongoing collaboration and capacity development.
- The joint development and approval of the 2022 Interim SSP in February 2022 to provide an updated framework for the Subsector's shared priorities going into the midterm election cycle.
- The development and coordination of regular security briefings available to election officials in all states and territories with DHS, the Federal Bureau of Investigation (FBI), and private sector owners and operators.

As Subsector collaboration has matured, the focus has shifted from developing new forums and establishing new relationships and processes to maintaining and utilizing those which have been built over the past several years. The GCC and the SCC work on an ongoing basis to help support election stakeholders with security and resilience activities, to identify needs and resources to address them, and to maintain an appropriate division of responsibilities with respect to the role of state and local governments as the responsible entities for election administration in the United States. As security risks to elections evolve into dynamic conditions, the Subsector continues to play a critical role in facilitating effective coordination on the security and resilience of U.S. election infrastructure.

This document was created as part of the Subsector’s GCC and SCC Joint Subsector-Specific Plan Working Group and documents guidance for the Subsector partnership through 2024. The Subsector recognizes the importance of its members approaching the 2024 election cycle with a shared interest in ensuring the security and resilience of sector personnel, assets, systems, and networks. These voluntary, collaborative efforts aim to boost collective capabilities for responding to incidents and to build resilience across the election ecosystem through coordinated information-sharing and risk mitigation for 2024.

The *National Security Memorandum on Critical Infrastructure and Resilience,* released April 30, 2024, updates national-level guidance related to protecting critical infrastructure. The National Security Memorandum (NSM) outlines how the U.S. Government will collaborate with key stakeholders to safeguard critical infrastructure, including partnering with relevant departments and agencies, the private sector and state, local, tribal, and territorial partners. The NSM mandates each Sector's SRMA, in consultation with the Sector's Councils, produce a sector risk assessment and sector risk management plan. Given the significant and ongoing efforts to address election infrastructure risks, CISA will work with the Subsector to develop and review the Subsector Risk Assessment in 2025, with subsequent updates planned for odd years. This new risk assessment will serve as the foundation for future updates to Election Infrastructure Subsector planning documents.

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

Information Sharing at the Classified and Unclassified Levels

Maintaining a robust information-sharing environment among election officials, private sector providers, and relevant federal partners continues to be a core focus for the Subsector. In the years since the critical infrastructure designation, the Subsector has established a mature framework for sharing cybersecurity threat and incident information. More recently, the GCC and the SCC have looked to these successes for lessons on how to improve information-sharing related to physical security threats. Subsector partners continue to collaborate on a voluntary basis to share actionable, relevant risk information; exchange best practices; build cross-sector situational awareness; and enable risk-informed decision-making.

The GCC recommended the establishment of the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) in 2018 to facilitate information sharing around cybersecurity risks. The EI-ISAC supports 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 surpassed 3,500 entities and continues to grow.

The EI-SIG, formed by voting system manufacturers working in partnership with the IT Information-Sharing and Analysis Center (IT-ISAC) in 2018, establishes industry-focused situational awareness, risk mitigation, and coordination capabilities through timely, reliable, and secure information-sharing. The EI-SIG serves as a primary vehicle for private sector training and security initiatives, including the adoption of organizational coordinated vulnerability disclosure (CVD) programs. The ongoing work of EI-SIG includes increasing membership and establishing sustainable processes for CVDs. In September 2023, the EI-SIG organized a pilot event focused on providing security researchers with access to voting technology under CVD principles.

Subsector members regularly receive threat information from the U.S. Intelligence Community through ISACs and other avenues, including classified and unclassified briefings. These briefings from DHS and its federal partners, including the 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 relevant classified briefings. CISA and its federal partners have worked with the GCC and SCC and their member organizations to improve the actionability of intelligence shared with the Subsector.

Although the State, Local, Tribal, Territorial, and Private Sector (SLTPS) Clearance Program helps ensure election officials have access to threat information, the Subsector continues 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.

Effectively sharing physical security threat information poses unique challenges. Because a potential threat to life may be present, the involvement of law enforcement is critical in responding to physical threats to a person or location. Sharing physical threat information nationally can be challenging because authorities governing response to threats related to election infrastructure and election officials vary across states and may be further complicated by difficulty understanding jurisdictional boundaries or overlap. Efforts to increase coordination within individual states, and to some extent at the federal level, have led to improvements in situational awareness about physical security threats to the Subsector. The GCC and the SCC continue to explore ways to further improve physical threat awareness while also ensuring election officials and private-sector partners understand their options for reporting physical security threats and incidents. Importantly, the Subsector repeatedly emphasizes the message that 911 should be the first call if an imminent threat to life is suspected.

In 2017, the GCC established protocols for election officials and their federal partners to report and share cybersecurity threat and incident information. As the Subsector has matured and federal partners have added additional field staff and resources, the opportunities for reporting and sharing information have increased in volume and complexity. To reflect this changing information sharing landscape, CISA issued new voluntary incident reporting guidance in July 2024, releasing 2024 General Election Cycle: Voluntary Incident Reporting Guidance for Election Infrastructure Stakeholders. This guidance provides examples of the threats and incidents election infrastructure stakeholders are encouraged to report and includes information about the Federal Government organizations to which stakeholders are encouraged to submit these reports.

The SCC updated its general guidance for incident reporting in 2021 and continues to utilize this framework subject to all other federal, state, and local requirements for such notifications. Additionally, CISA is expected to produce a notice of proposed rulemaking for incident reporting for entities in critical infrastructure sectors under the Cyber Incident Reporting for Critical Infrastructure Act by March 2024.

CISA, FBI, and the EI-ISAC remain committed to timely victim notification if they become aware of a potential incident impacting election infrastructure. In accordance with their policies, these entities will notify the appropriate state election official and local election official (if a local incident). State election officials are responsible for making further notifications as they deem appropriate.

Risk Management for Physical and Cyber Security

Coordinating cybersecurity and physical security risk management across election stakeholders and supporting entities is an ongoing key priority for the Subsector. This includes consideration for threats associated with generative artificial intelligence, which has the potential to exacerbate existing risks to election infrastructure by increasing the speed and sophistication of cyber threats and false information. Through this partnership, the Subsector has developed tools, resources, and programs that support sector-wide risk management and maximize resources. Key examples include conducting vulnerability assessments, developing threat briefings, holding tabletop and training exercises, and collaborating with state and local election authorities to strengthen disaster and emergency response plans.

The GCC and the SCC continue to focus on increasing the availability and use of resources and services from CISA, EI-ISAC, and others. Both Subsector Councils provide ongoing feedback to federal partners on the resources they provide and where the Subsector has additional needs. For example, as election-related facilities have become an increased focus of potentially threatening activities, the Subsector has identified the need to expand the availability and use of resources that will help election officials and industry partners secure their physical locations.

A recent example is the November 30, 2023, joint FBI/U.S. Postal Inspection Service (USPIS) advisory providing notice and awareness of suspicious letters (at least one containing fentanyl) sent to election offices across the U.S. in early November. This activity constituted attempts to disrupt U.S. election processes and intimidate election workers. Working with the USPIS, the EI-ISAC distributed resources on election mail, including guidance for mail center security and handling suspicious mail pieces to the election community.

Engagement with the GCC and the SCC has also helped CISA scale and tailor its cybersecurity and physical security services to meet the needs of election stakeholders. Through the Subsector Councils and their member organizations, CISA is able to encourage the use of services and resources ranging from cybersecurity assessments to incident response on the cyber side, and including training, written resources, and assessments on the physical side. Due in part to increased demands and a challenging political environment, the Subsector is currently dealing with widespread turnover of election officials and employees. As such, keeping resources updated and promoting these resources and services on an ongoing basis remains a priority.

Thanks to strong interest and feedback from both government and private sector stakeholders, CISA is promoting a more scalable model of cybersecurity service delivery through which increasingly intensive services become available as election entities progress through foundational assessments. CISA is similarly exploring opportunities to reach more election entities with physical security support by training election officials and other stakeholders to perform assessments currently conducted by CISA employees (a train the trainer model) and by creating targeted resources for election entities such as Physical Security of Voting Locations and Election Facilities.

Part of CISA's more scalable service model includes building up its regional staff to deliver services in the field and promoting the use of services available through the EI-ISAC. CISA has hired Election Security Advisors in each region with the goal of optimizing how election officials engage with CISA services and regional personnel.

The EI-ISAC services, including Malicious Domain Blocking and Reporting (MDBR) and Endpoint Detection and Response, continue to add value, particularly to small election jurisdictions that may not have sufficient local resources. Additionally, the EI-ISAC recently fully-launched a Vulnerability Disclosure Program, building upon a previous pilot program, to make additional support available to state and local election entities as they expand their coordination with security researchers. A current area of focus for the GCC is planned coordination with EI-ISAC leadership throughout 2024 to ensure a robust information-sharing environment across federal partners and to help expand the utilization of EI-ISAC services.

The Subsector Councils also provide opportunities for election stakeholders to collaborate with cybersecurity companies. In 2022, CISA collaborated via its Joint Cyber Defense Collaborative with public and private sector partners to release the Cybersecurity Toolkit and Resources to Protect Elections which outlines free tools, services, and resources available from CISA and private sector cybersecurity partners to election stakeholders. Updates to the Toolkit are anticipated for 2024.

The Subsector continues to work with CISA and other partners to identify cybersecurity and physical security topics where new resources are needed. An example is A Guide to Mitigating Risks of Denial of Service released in September 2023. Further, the GCC and the SCC also contribute to and promote resources on topics that support both cybersecurity and physical security resilience such as incident response preparedness, insider threat mitigation, and chain of custody best practices. A GCC-related example includes CISA's continued collaboration with state and local election offices to expand their Last Mile initiative. Through this initiative, CISA and election jurisdictions 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.

Election officials operate under the highest levels of public access and transparency, which makes the challenge of balancing security needs with these principles particularly pronounced for the Subsector. Election officials across the country are dealing with an influx of public records requests that have only increased in number and complexity since 2020. While promoting transparency and complying with public records laws is critical, it can also create capacity/resource challenges due to the time required to respond to records requests. In some cases, it can also lead to security concerns when disclosure of certain technical or security-related information about an election technology used in one jurisdiction could potentially put other jurisdictions that use that same technology at risk. The sheer number of requests means that a malicious actor could use public disclosures from multiple sources to assemble a picture of an election office's security profile.

Each entity receiving a public records request will need to determine whether records are subject to disclosure under their own state law, including whether any identified responsive records may be subject to information protections in federal law. For example, the Cybersecurity Information Sharing Act of 2015 (CISA 2015) creates protections for cyber threat indicators and defensive measures shared in accordance with the statutory requirements with state and local entities, including that the information shall be exempt from disclosure under state and local freedom of information laws. Critical Infrastructure Information is protected under CISA's Protected Critical Infrastructure Information (PCII) Program if it meets a number of procedural requirements. Like CISA 2015, the PCII Program also provides protections for sharing entities, including exemption from disclosure under state and local freedom of information laws. The Subsector Councils are currently focused on ensuring that all stakeholders are aware of these programs.

Subsector organizations continue to progress efforts to support the ongoing security and resilience of U.S. elections. Examples include the further adoption and expansion of both coordinated vulnerability disclosure and election technology testing programs by state and local election entities and private-sector technology providers. The Subsector provides forums to coordinate and promote these efforts.

It is important to note that election offices and industry partners engage in extensive cybersecurity and physical security risk management activities to create their own internal plans. In addition to support from the federal government, election stakeholders collaborate with other state or local agencies, the private sector, academia, and others on continuous improvements to their security and resilience. When owners and operators better understand their risks and interdependencies, they can develop strong business continuity strategies that build agility and redundancy into operations and implement security practices that mitigate risks to personnel, facilities, systems, and other assets.

Cross-Sector Risk Management

Like many other sectors and subsectors, the Election Infrastructure Subsector is dependent on infrastructure and services provided by other sectors, including Information Technology, Communications, Emergency Services, Energy, Government Services and Facilities, Commercial Facilities, and Transportation, among others. Significant or prolonged outages impacting these sectors around critical election deadlines or process benchmarks may exceed an individual election office's ability to respond or function, and the Elections Subsector may not be top-of-mind for an impacted sector, especially if the impacted sector/entity is not already aware of the election calendar or the criticality of the dependency. Furthermore, many dependent sectors cross jurisdictional lines, including, in some limited cases, international boundaries.

Individual election entities can take proactive steps to manage risk to their operations associated with disruption or lack of availability of some of these dependencies, including engaging in ongoing conversations with local service providers and building redundancy into processes wherever possible. However, cross-sector dependencies may be more efficiently addressed at the state or territory level, with assistance from CISA.

CISA is currently undertaking an update to their 2020 Elections Subsector Risk Assessment, conducting a cross-sector risk analysis to provide a baseline for the impact other sectors could have on the Elections Subsector. This important first step will allow both election officials and their private sector partners to have risk-informed conversations with relevant providers within their jurisdictions and will help the Subsector Councils engage in risk-informed conversations with their counterparts in other sectors.

Managing Risks to the Supply Chain

The federal government has prioritized efforts to raise awareness around the risks associated with industry supply chains. Supply chain risk management is necessary to ensure election officials and their supply chain partners only procure election-related paper products, software, hardware, and services from legitimate sources that have a program in place to ensure supply chain integrity. 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 SCC leaders to keep industry partners apprised of their progress and accept elections SCRM input.

In June 2021, the SCC established a 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 ballot paper and envelopes, software, hardware, and services to assess and reduce risks to the election jurisdiction and their supply chain partners.

In January 2024, the SCRM Subgroup on Ballot Paper issued a white paper that provides an updated assessment and risk mitigations for subsector partners regarding the ballot paper and envelopes supply chain. The SCRM Subgroups on hardware, software, and services also released an additional white paper in January 2024 that serves as a resource to assist election technology providers and election officials when procuring election-related software, hardware, and services. The document also provides updated guidance on how organizations and downstream supply chain partners, including election officials, can better secure their hardware, software, and services supply chains. The collection of publications provides the following information related to election supply chain risk management:

- SCRM Working Group guidance on procurement for election related supply chain risk management;
- Existing resources provided by CISA and the ICT SCRM Task Force;
- Checklists and other resources that technology providers and election officials may use to assess their election supply chain risk management strategy;
- Resources through the election community to increase awareness of supply chain risk management practices.
- Complementary work by other federal agencies such as the Election Assistance Commission's Voluntary Voting System Guidelines (VVSG) version 2.0 that strengthens supply chain risk management process and reporting requirements on voting technology providers. Although no VVSG 2.0 systems will be certified or in use for the 2024 presidential election, this work will buttress supply chain risk management in future voting technology.

Promoting Accurate Information and Countering False Information

False or misleading information about election administration poses risks that can interfere with the administration of safe and secure elections. Actors with malicious intent, including foreign adversaries, have promoted false information to intentionally confuse voters and undermine confidence in the election process.[1] False information is often spread inadvertently, but still causes confusion, for example, by misleading voters on when or where to vote in their jurisdictions. A lack of understanding about the election process makes individuals more susceptible to believing inaccurate information, and false information can lead to mistrust of the people, processes, and technologies responsible for the administration of elections. Regardless of whether it is intentional or inadvertent, false information has resulted in threats or violence against election workers, officials, and private sector partners.

[1] 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.

Election officials, industry providers, and other organizations associated with the Subsector have implemented initiatives to promote accurate information-sharing about elections to increase the public's overall understanding of election processes. For example, the National Association of Secretaries of State (NASS) launched the #TrustedInfo public education effort in November 2019 to encourage voters to get election information directly from election officials. Returning for the upcoming elections, the #TrustedInfo2024 initiative promotes common messaging strategies across state elections offices and directs voters to the websites of their state and local election officials through NASS's nonpartisan site, CanIVote.org. Another example, the National Association of State Election Directors (NASED) developed an Election Communications Toolkit with customizable graphics to make it easier for election officials to proactively communicate with their voters and drive traffic to election office websites; the Toolkit includes elections-specific media literacy tipsheets developed with the National Association for Media Literacy Education to help election officials educate key audiences about using media literacy principles to understand the information they consume about elections. NASED also developed a high-level Frequently Asked Questions page in both English and Spanish that directs users to state and territorial websites, as well as to national resources like the EAC, CISA, and National Conference of State Legislatures.

Since CISA developed a Rumor vs. Reality webpage in 2020, many government and private elections-focused entities have produced similar webpages. The GCC and SCC have identified and shared guidance with election stakeholders to help them take steps like establishing websites to provide accurate information about election administration, technology, and security and to dispel false information and voter confusion. Efforts like these are expected to expand across the Subsector for 2024, as the Subsector innovates on tactics and tools to educate voters and other key audiences.

The Subsector has also promoted adoption of the .gov web domain for helping the public identify official election resources, as .gov domains are available exclusively to U.S. federal, state, local, tribal, and territorial, or other publicly-controlled entities. As of April 2021, the .gov program is administered by CISA and is available to U.S.-based government organizations at no cost.

Personnel Security

As noted by CISA in a 2022 publication entitled, Personal Security Considerations, "The U.S. continues to face a dynamic threat environment for targeted violence towards individuals or organizations that epitomize personal, political, or ideological grievances. This is further exacerbated by misinformation campaigns that aim to sow discord, shape public sentiment, and even encourage violence against individuals." The DHS 2024 Homeland Threat Assessment anticipates this trend will continue, with potential for violence or threats directed at government officials, voters, and elections-related personnel and infrastructure.

In recent years, election workers in both the public and private sectors have become the subject of hostile communication and unfounded theories, leading to doxing, physical stalking, intimidation, threats, and more. This focus on individuals has put members of the elections community and their families at risk.

CISA created resources on doxing mitigations to help Subsector partners protect their personal information before it can be made public. The only way to prevent doxing is to make it difficult to find personally identifiable information and details online. Moving into 2024, members of the Subsector should consider:

- Conducting a social media audit of themselves to deactivate or delete unused accounts, removing personally identifiable information from accounts, and implementing security controls on all accounts, including two-factor authentication;

- Reviewing public records websites, often known as data brokers, that post personally identifiable information, and requesting personal information be removed; and
- Discussing with family and friends what information and images they are and are not comfortable with being shared on the Internet.

The EAC created a webpage aggregating information for election officials experiencing threats, including mental health resources.

FBI Election Crimes Coordinators (ECCs), who are already placed in all 56 FBI field offices as the primary points of contact on election crimes, now also intake hostile communication for triage from election offices on behalf of the Task Force on Threats Against Election Workers. USPIS also has Election Crimes Coordinators across the country who help members of the Subsector address suspicious mail, including threats and harassment received via postal mail. Many state election offices are working with their state law enforcement agencies to develop robust in-state networks with clear reporting protocols to leverage state/territorial legal frameworks. Many local election offices have also established year-round relationships with local law enforcement through trainings, going beyond the traditional engagement specifically tied to the election calendar.