



# Election Infrastructure Subsector Specific Plan

An Annex to the NIPP 2013

2018



Homeland  
Security

# TABLE OF CONTENTS

Election Infrastructure Subsector Government Coordinating Council Letter of Support	ii
Executive Summary	iv
1 Introduction	1
2 Subsector Overview	2
2.1 Subsector Profile	2
2.2 Subsector Risks	5
2.3 Election Infrastructure Partners	6
3 Election Infrastructure Risk Management	8
3.1 Risk Management	8
3.2 Bolstering Risk Management Capabilities	8
4 Vision, Mission, Goals, and Priorities	10
5 Subsector Activities and Measuring Effectiveness	12
APPENDIX A. Government Coordinating Council Member Profiles	14
APPENDIX B. Subsector Coordinating Council Members	16
APPENDIX C. Risk Management and National Preparedness	17
APPENDIX D. Glossary of Terms	24
APPENDIX E. Acronyms and abbreviations	26

# ELECTION INFRASTRUCTURE SUBSECTOR GOVERNMENT COORDINATING COUNCIL LETTER OF SUPPORT

In January 2017, the Federal Government established the Election Infrastructure Subsector (EIS) as a critical infrastructure sector in the United States, recognizing that its security and resilience is essential to maintaining free, fair, and secure elections. Since that time, the Subsector has established partnerships among government stakeholders at the federal, state, and local levels and between the public and private sectors, forming both a Government Coordinating Council (GCC) and Subsector Coordinating Council (SCC). These partnership organizations are collaborating with the U.S. Department of Homeland Security (DHS), law enforcement, and the intelligence community to enhance information sharing about risks to our election systems, identify resources to help mitigate such risks, communicate best practices, address identified vulnerabilities, and enable election officials' access to classified threat information. State and local governments have engaged federal counterparts, other state agencies, and the private sector with the intent of conducting vulnerability assessments on election systems and increasing the focus on the cybersecurity of election systems.

## Subsector-Specific Plan

The *Election Infrastructure Subsector-Specific Plan* (SSP) describes a collaborative approach among the private sector; federal, state, local, tribal, and territorial (SLTT) governments; and non-governmental organizations (NGOs) to reduce risks to the Nation's election infrastructure. The mission, vision, and goals described in the SSP set the strategic direction for the EIS and provide important information on the EIS and risk management approaches to enhance election infrastructure security. The Subsector's goals focus on communication, capacity building, and access to resources. The SSP describes activities and timelines in support of achieving Subsector priorities.

## Accessing Subsector Resources

The SSP is intended to educate EIS stakeholders and communicate goals and objectives for ensuring the security of election systems. The Nation's attention and resources are focused on election security. Sharing information with the public and other stakeholders is a priority for the Subsector, and the latest information for election officials and other sector stakeholders is available at <https://www.dhs.gov/topic/election-security>.



**Robert Giles**

Director of Elections, New Jersey



**Thomas Hicks**

Chairman, U.S. Election Assistance Commission



**Bob Kolasky**

Assistant Secretary (Acting), Office of Infrastructure  
Protection U.S. Department of Homeland Security



**Connie Lawson**

Secretary of State, Indiana



**Noah Praetz**

Director of Elections, Cook County, Illinois

# EXECUTIVE SUMMARY

In January 2017, the Secretary of Homeland Security designated the Nation’s election infrastructure as critical infrastructure, making it a subsector of the Government Facilities Sector. The *Election Infrastructure Subsector-Specific Plan* (SSP) outlines actions for how the U.S. Department of Homeland Security (DHS), the Government Coordinating Council (GCC), and the Subsector Coordinating Council (SCC) will support the owners, operators, and stakeholders of the Nation’s election infrastructure to ensure secure and resilient election systems.

Election officials have always recognized the risks to election systems. Historically, these have included human, physical, and natural hazards and required balancing access and security to manage. Although physical security remains important, cyber risks have rapidly increased and evolved. The Election Infrastructure Subsector (EIS)—like other sectors and institutions—has leveraged digital technology to improve speed and efficiency at a time when malicious actors are increasing their capacity and intention to disrupt business as usual. However, cyber risks are more pronounced for election infrastructure, which has operating environments across multiple governance models, distributed but inter-reliant systems, and limited resources. In addition to these challenges, the EIS also recognizes that the mere perception of a disruption or incident could result in the erosion of public trust in elections. Free and fair democratic elections are the foundation of the American way of life, and despite the remote risk, the successful exploitation of election infrastructure could prove disastrous to the public’s confidence in election officials and election outcomes.

## Election Infrastructure Subsector Assets and Risks

**ELECTION SYSTEMS** include infrastructure to manage voter registration, planning and execution of elections, counting and reporting of election results, and other software and hardware used by election officials.

Elections are managed and administered across thousands of jurisdictions at the state and local levels of government, leading to a vast range of infrastructure and administrative policies. The Subsector is composed of assets, systems, and networks that contain physical, digital/cyber, and human components. The Subsector includes systems to manage voter registration, planning and execution of elections, and counting and reporting of results.

The Subsector’s diversity in organization, systems, networks, and assets diffuse some risk for federal and statewide elections away from a single point of failure; but a smaller political or legislative district contained in a single election jurisdiction may create significantly more risk of a material effect on the actual

outcome of local races, if not for carefully organized audit and recount procedures. To manage risks throughout the Subsector, partners collaboratively undertake the critical infrastructure risk management framework process. The EIS risk management process entails identifying critical infrastructure, assessing and analyzing risk, and implementing informed risk management activities. Information is shared throughout the process to facilitate decision-making, and to document and continue to develop best practices and lessons learned on how to identify and address gaps in security and resilience efforts. Federal, state, and local capabilities and resources are brought to bear to support election infrastructure resilience, including risk management processes and information sharing.

## Election Infrastructure Subsector Partnerships

Collaboration in the EIS occurs between the GCC, made up of federal, state, and local officials, and the SCC, which is made up of private sector stakeholders. This partnership, facilitated by DHS as the Sector-Specific Agency (SSA), enables collaboration to develop tools, resources, and programs that support sector-wide risk management and maximize partners’ limited resources.

## Subsector Goals, Priorities, and Activities

As part of this 2018 SSP, the EIS has coalesced around a common mission and vision, and identified goals and priorities to guide the Subsector’s security and resilience efforts. The EIS developed a slate of activities and milestones under the following overarching goals:

The Election Infrastructure Subsector Government Coordinating Council **MISSION** is to coordinate and advocate state and local election administration perspectives and needs across the spectrum of infrastructure service providers, governmental partners, funders, supporters, and other stakeholders.

- Ensure actionable, timely information sharing and consumption throughout the Subsector to promote clear information about security threats, probabilities, vulnerabilities, controls, and responses.
- Support efforts that will increase election officials' capacity to defend against, detect, and recover from security incidents and ensure a common understanding and approach to building resilience.
- Work to establish consistent sources of appropriately flexible funding that will support the Subsector's cyber resilience and national security efforts.

The focus of these goals, objectives, and activities highlights the Subsector's evolving risk profile, capabilities, and needs. Predominant themes include: building capacity, with an emphasis on cybersecurity; developing incident response plans and playbooks; and increasing information-sharing capabilities and requirements. The objectives, activities, and metrics included in the 2018 SSP guide the EIS security and resilience efforts, inform decision-making, and reflect actionable activities that Subsector partners can pursue to reduce election infrastructure risks and improve risk management practices, taking into consideration the unique risk management perspectives and resource constraints of the subsector.

The **VISION** of the Election Infrastructure Subsector Government Coordinating Council is to provide a unified government approach to enhance security and resilience efforts to ensure secure elections.



# 1 INTRODUCTION

In January 2017, based on the vital role elections play in the United States, the Secretary of Homeland Security designated election infrastructure as a critical infrastructure subsector under the Government Facilities Sector. 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. Federal, state, and local officials as well as the private sector all have roles to play in protecting elections from a variety of threats. The critical infrastructure designation will augment state and local governments' existing election security efforts on a more formal and enduring basis by ensuring that election infrastructure will be a priority for the assistance and protections that DHS can provide for cyber and physical infrastructure.

This 2018 Election Infrastructure Subsector-Specific Plan (SSP) is designed to guide voluntary, collaborative efforts to improve security and resilience in the Election Infrastructure Subsector (EIS). Most importantly, this SSP sets the Subsector's strategic direction by identifying shared goals, priorities, and activities for Subsector partners. The SSP identifies collaborative approaches to manage EIS risks in the face of limited resources while not altering or impeding the ability of EIS partners to perform their respective responsibilities under the law.

In addition to this introduction as Chapter 1, this SSP includes the following sections:

- **Chapter 2:** Subsector Overview – Provides a concise description of the Subsector's major components, risk profile, organizational structures, and partners.
- **Chapter 3:** Election Infrastructure Risk Management – Describes the Subsector's mechanisms to achieve its goals, specifically the sector's risk management approach, including collaborative programs, activities, and resources; approaches to cybersecurity; and efforts to leverage research and development (R&D).
- **Chapter 4:** Vision, Mission, Goals, and Priorities – Presents the Subsector's vision for security and resilience, the mission to enact that vision, and updated goals and priorities to support the [National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience \(NIPP 2013\)](#) goals and Calls to Action, and the [2014 Joint National Priorities for Critical Infrastructure Security and Resilience](#).
- **Chapter 5:** Subsector Activities and Measuring Their Effectiveness – Lists the specific activities the EIS plans to undertake in partnership to address Subsector priorities and describes the approach the Subsector will use to measure the effectiveness of individual activities.
- **Appendices:** Provides additional detail to support the major chapters of this SSP, including sector membership, glossary of terms, references, and detailed information on risk management.

This SSP is a living document and will be updated periodically to reflect changes in national policy and plans, lessons learned, Subsector composition and structure, industry collaboration, and priorities of Subsector stakeholders.

# 2 SUBSECTOR OVERVIEW

This chapter profiles the Subsector’s design and operating characteristics; identifies its primary risks and interdependencies; and describes how the Subsector’s public-private partnership operates.

## 2.1 Subsector Profile

The EIS includes all election-related functions, facilities, and systems, including voter registration and election management. Almost the entire set of policies and laws that dictate how elections in the United States are managed are set forth by the states and territories.<sup>1</sup> The Federal Government’s role in elections is limited to a number of constitutional thresholds, including the Fourteenth,<sup>2</sup> Fifteenth,<sup>3</sup> Seventeenth,<sup>4</sup> Nineteenth,<sup>5</sup> Twenty-fourth,<sup>6</sup> and Twenty-sixth Amendments,<sup>7</sup> all of which guarantee access. Laws that limit the Federal Government’s role include the Civil Rights Act,<sup>8</sup> the Voting Rights Act of 1965,<sup>9</sup> the National Voter Registration Act (NVRA),<sup>10</sup> the Help America Vote Act (HAVA),<sup>11</sup> and the Military and Overseas Voter Empowerment Act of 2009.<sup>12</sup>

Each state and territory has a chief election official charged with ensuring compliance with policies and laws. Since HAVA became law in 2002, states have the major responsibility for maintaining and managing the list of registered voters. Many jurisdictions also have their own rules that apply only to local elections. Although some states play a larger role by managing and maintaining much of the election infrastructure, including voting equipment, nearly 9,000 local election officials at the county or municipal level maintain and manage the majority of the election infrastructure in the United States. Additionally, many of these local election officials depend on third party providers to conduct day-to-day management of election infrastructure due to budget constraints and staffing challenges in the face of a broad portfolio of responsibilities.

### Key Subsector Operating Characteristics



**Election administration is highly decentralized, but deeply interrelated.** There are thousands of local election officials and hundreds of thousands of poll workers, election judges, and election staff; but all elections draw from state databases of registered voters and many draw on the same technology resources and providers.



**Elections occur throughout the year.** Election administrators at both the state and local level devote significant time and money in pre-election activities to prepare for each election. Similarly, elections do not end on Election Day; there is significant post-election reporting and activity for every election.



**Election administration affects every facet of government.** Voter confidence in an election outcome is critical to peaceful transition of power. Any incident, regardless of how minor or isolated, can have long-term negative consequences on voter turnout, civic engagement, and trust in government. When voters lose confidence in the process, they lose confidence in the results.

<sup>1</sup> U.S. Const. Art. I.

<sup>2</sup> U.S. Const. Amend. XIV.

<sup>3</sup> U.S. Const. Amend. XV.

<sup>4</sup> U.S. Const. Amend. XVII.

<sup>5</sup> U.S. Const. Amend. XIX.

<sup>6</sup> U.S. Const. Amend. XXIV.

<sup>7</sup> U.S. Const. Amend. XXVI.

<sup>8</sup> Civil Rights Act of 1964, Pub. L. 88-352, 78 Stat. 241 (1964), <https://www.gpo.gov/fdsys/pkg/STATUTE-78/pdf/STATUTE-78-Pg241.pdf>.

<sup>9</sup> Voting Rights Act of 1965, Pub. L. 89-110, 79 Stat. 437 (1965), <https://www.gpo.gov/fdsys/pkg/STATUTE-79/pdf/STATUTE-79-Pg437.pdf>.

<sup>10</sup> National Voter Registration Act (NVRA) of 1993, Pub. L. 103-31, 107 Stat. 77 (1993), <https://www.gpo.gov/fdsys/pkg/STATUTE-107/pdf/STATUTE-107-Pg77.pdf>.

<sup>11</sup> Help America Vote Act (HAVA) of 2002, Pub. L. 107-252, 116 Stat. 1666 (2002), <https://www.gpo.gov/fdsys/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf>.

<sup>12</sup> Military and Overseas Voter Empowerment (MOVE) Act, H.R. 2647, Pub. L. 111-84, 123 Stat. 2190 (2009), <https://www.fvap.gov/uploads/FVAP/Policies/moveact.pdf>.

# ELECTION INFRASTRUCTURE SUBSECTOR SNAPSHOT

## COMPONENTS



## PRIMARY ACTORS

 Federal and SLTT governments

 Non-profit organizations

 Membership organizations

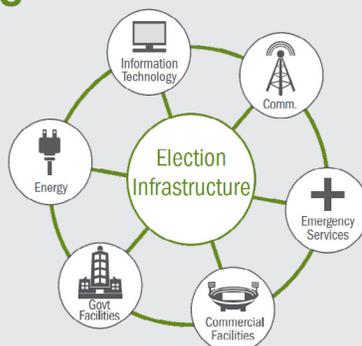
 Academia

 Election technology vendors & other commercial entities

 Temporary/seasonal volunteers

 Third party/Outside agency support positions

## CRITICAL SECTOR DEPENDENCIES



## Subsector Components and Assets

The U.S. Department of Homeland Security (DHS) designation of the EIS identifies election infrastructure as the physical locations, information and communications technologies, and personnel used to conduct elections. In line with this designation, the EIS categorizes the Subsector's components into the categories of physical, digital/cyber, and human. The following is a list of Subsector components and assets:

### Key Physical Components

Equipment and materials, facilities, and records that support or provide protection for the EIS.

- **Voting Locations** – Facilities used by election officials to enable voters to cast ballots in person, which is a significant proportion of total votes. Continuity of the voting process is dependent on the availability of voting locations and their ability to provide security and any other systems required to operate the voting process.
- **Technical Facilities** – Facilities used to house servers and network equipment. This can be a mix of onsite, offsite, or co-located facilities. There may also be facilities used to process vote tallies and ballot creation systems.
- **Storage Facilities** – Facilities, including warehouses or other similar facilities, used to house equipment and ballots that require high levels of security.

- **Processing Facilities** – Facilities used to print ballots, sample ballots, or polling place supplies. These facilities are either onsite or at a contractor’s facility and must have adequate security and protection from the elements to ensure voting processes continue.
- **Voting Hardware** – Ballots, poll books, machines, and records as well as the physical equipment supporting digital systems that must be stored securely and protected.

## Key Digital (Cyber) Components

Hardware and software components critical to supporting the EIS mission, including computers, servers, databases, and other information technology (IT) systems and assets used in EIS activities to fulfill one of the following roles:

- **Voter Registration Systems** – Systems used to collect personal voter information and the information required to determine voter eligibility. The systems are also required to prevent duplicate voting. These systems are maintained at the local jurisdiction level, the state level, or a combination of both. The data on these systems must be readily available and maintain data integrity.
- **Election Management Systems** – Systems used to manage the entire voting process, which can include addresses, precincts, political and taxing districts, contest parameters, poll workers, voters, voting, candidates, and ballot layout.
- **Voting Systems** – Systems used to record votes, then accumulate and present them. Votes may be recorded on paper, directly onto voting machines, or both, including through Direct Recording Electronic (DRE) machines, or optical scanners used to cast paper ballots marked by hand or with a Touch Screen Ballot Marking Devices (TSBMD). Regardless of the method, the voting system has a digital/cyber component because the ballots must be counted on a digital/cyber component at some point. Voting systems typically consist of centrally located components for ballot creation, creation of machine programming and directional files, and vote counting, in addition to the machines used by voters to cast their ballots.
- **Results Reports** – Election-night reporting systems used to generate and display unofficial results. These systems can be online systems, locally hosted systems, or a combination of both. These systems operate by uploading count data to the program, which then displays those totals in relationship to the overall population of a given jurisdiction. The integrity of the unofficial results must be maintained at all times because candidates and the public rely on election night reporting to provide accurate and timely information.
- **Public Information Systems** – Systems to provide the public with general information about the election process, upcoming elections, and election results. The systems can also provide individual-level information regarding registration status, provisional ballot status, mail ballot status, voting location, or support blank ballot delivery.
- **Electronic Poll Books** – Systems used by workers to identify eligibility of voters and the correct ballots to provide them. Some electronic poll books even allow jurisdictions to update voter records or register voters for the first time. Electronic poll books contain the list of voters used by election workers. They must be readily available in order for the voting process to continue without resorting to paper based mitigations. Levels of connectivity vary, and this determines the risk profile of specific platforms.
- **Internal Production Software and Servers** – Various software platforms and servers that support the EIS environment. This includes but is not limited to geographic information systems (GIS), which support the creation and assignment of eligible voters into various political and election-specific subdivisions. These systems must remain accurate to ensure voters receive the correct elections materials.

## Key Human Components

Personnel with unique training, certification, knowledge, skills, authorities, or roles whose absence could cause undesirable consequences or hamper the EIS mission.

- **Strategic Positions** – Elected and appointed officials at the state and local level, such as local election officials, state election directors, Secretaries of State, and others who often make up the leadership of the EIS.
- **Operational Positions** – Individuals who operate election systems and have in-depth understanding of their functionality. Their subject matter expertise ensures the operability of equipment. This includes operators of voting systems, voter registration systems, electronic poll books, election websites, election night reporting, phone systems, and other systems and equipment.

- **Temporary/Seasonal Positions** – Individuals selected on a short-term basis to carry out specific tasks within the EIS and are essential to the ability to conduct elections. This includes temporary office staff and poll workers.
- **Third Party/Outside Agency Support Positions** – Individuals outside the direct supervision of election officials who support election systems and other digital/cyber and physical assets essential for the conduct of elections. This includes providers and personnel from other agencies both within and outside the jurisdiction.

## 2.2 Subsector Risks

### Notable Trends and Emerging Issues

Elections have always been high value targets, with numerous examples across American history of people manipulating or ignoring the rules to influence the outcome in favor of a preferred result.

The industry’s migration to digital/cyber technologies has created a new challenge as malicious cyber actors have shown an intent to exert influence over election systems. This growing threat has created increased security concerns that must be assessed and managed by election officials.

The changing and often unpredictable nature of both cyber and physical threats to election infrastructure is an ever-evolving challenge. Facilitating the democratic process for the public requires EIS partners maintain a high level of threat awareness, as well as the capacity to respond to an increasing number of complex challenges.

### Significant Election Infrastructure Risks

Election officials manage or rely on multiple environments to operate election systems. These environments can be roughly divided into three categories:

- a disconnected environment where materials and information are shared on paper and there is minimal use of technology;
- a semi-connected environment where digital/cyber technologies are relied upon, but they are not connected directly to a network, thereby actively protected from broad risks of connectivity, because removable media is used to load information and protocols; and
- a fully connected environment where the advantages of networking are relied upon to connect devices to further the service offerings of election systems.

Compared to paper-based elections, the latter two digital/cyber environments provide capabilities that enhance the efficiency of elections but are comparatively more vulnerable to the modern threat environment.

Election officials embrace an all-hazards approach to protecting the election infrastructure. However, each elections agency operates with varying constraints, including geography, authorities, prioritized risk areas, levels of technology, and resource limitations. The information below represents the most common significant risk areas that elections agencies manage to ensure security and resilience. Since these risks occur frequently across jurisdictions, they can be considered national-level risks.

#### Digital/Cyber

Cybersecurity of election infrastructure is exceedingly complex with risks facing both election-related activities and day-to-day management, such as voter registration. Election agencies consider a multitude of emerging issues to manage cyber risks.

The interpretation of cyber resilience varies among agencies and the cyber-risk environment is based on each entity’s infrastructure vulnerabilities and security capabilities, which can vary widely from jurisdiction-to-jurisdiction. However, certain cyber issues are common across jurisdictions. These include:

- cyber-physical system dependencies,
- increasing dependence on technology,
- potential cyber vulnerability exploitation by nefarious actors,
- information systems access control,
- information security deficiencies, and
- personnel and knowledge gaps.

The complexity of system dependencies and emerging risks can create cascading effects from a cyber incident beyond the initial target to additional systems. Containing the cascading effects of a cyberattack may be complicated by information-sharing barriers and the evolving nature of cyberattack vectors (e.g., information security breaches, hacking, phishing, and malware). Successfully securing cyber systems relies on the timely sharing of information (e.g., threat, incident, and response capability) between public and private sector stakeholders.

### Physical

Soft targets are sites that are more vulnerable to attack, compared to hardened facilities, due to their open access and limited security barriers. Soft targets include office facilities and voting locations (e.g., early voting sites, Election Day polling places, ballot drop boxes, and vote centers). Many voting locations pose a particular challenge because of the need to ensure accessibility and ease of use for voters and poll workers to avoid discouraging voter participation. This can be further complicated by the fact that polling places are often located at schools, community centers, or other publicly accessible facilities that are more difficult to secure. Some states and jurisdictions have laws that limit police presence at these locations, which limits options to manage physical risks. Implementation of security best practices can help mitigate broader physical security risks, but access control through the physical protection of network and election hardware is also needed to manage cyber vulnerability.

## Cross-Sector Dependencies

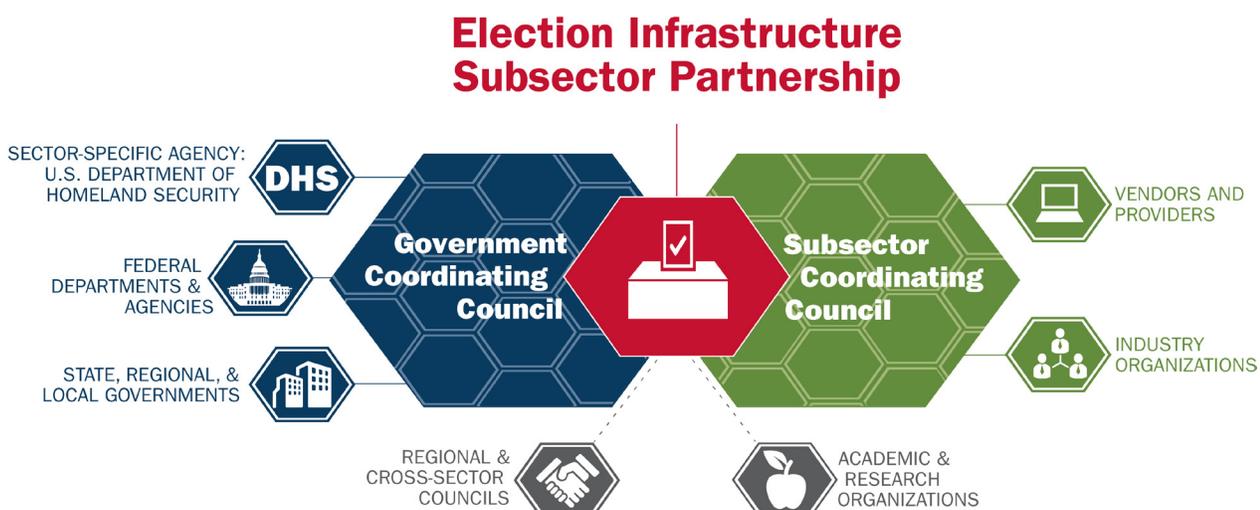
To varying degrees, elections are run on top of infrastructure already broadly supported and protected under the critical infrastructure designation. Election systems use Communications, Commercial Facilities, Government Facilities, Energy, Emergency Services, and Information Technologies sectors. A disruption to these other critical infrastructures can affect election-related activities, but the Subsector has the capability to continue operations in the face of these degradations. Overall, the EIS will place priority on addressing inherent risks from use of information technology in election activities.

## 2.3 Election Infrastructure Partners

Ensuring security and resilience requires an engaged whole community—federal and state, local, tribal, and territorial (SLTT) governments, membership organizations and associations, election technology providers and other commercial entities, non-profit organizations, and academia. Government constituents include the federal, state and local government agencies (and organizations representing government officials) that own, operate, or administer physical or digital/cyber assets, systems, and processes to conduct elections, or have responsibility for supporting the security and resilience of those assets, systems, and processes.

A variety of private sector stakeholders are involved in election-related activities. Election technology providers, who provide the systems and machines that facilitate the process of voting from voter registration through post-election counting and auditing. Media organizations provide the public election results. Non-partisan, non-profit organizations fill numerous roles, including support of voter participation through assisting with registration, analysis of registration data, finding voting locations, providing security best practices, convening experts, and advocating for secure democratic processes.

Figure 1. Election Infrastructure Subsector Partnership Structure



## Sector-Specific Agency

DHS is the designated Subsector-Specific Agency (SSA) for the EIS. DHS coordinates partnership activities and information sharing and, for security and resilience, is the primary federal interface with Subsector stakeholders. The Office of Infrastructure Protection (IP) fulfills the role of SSA for DHS with the Assistant Secretary of Infrastructure Protection as a member of the EIS Government Coordinating Council (GCC) Executive Committee.

## Election Infrastructure Subsector Government Coordinating Council

The EIS GCC enables federal, state, and local governments to share information and collaborate on best practices to mitigate and counter threats to election infrastructure. The GCC consists of 24 state and local government representatives and 3 federal government representatives. The GCC, governed by an operating charter, held its first meeting on October 14, 2017, and will convene at least twice a year.

## EIS GCC Executive Committee

The EIS GCC formed an executive committee of five member organizations to drive action on priorities between meetings. Those members include the DHS IP Assistant Secretary, the Chair of the Election Assistance Commission (EAC), the President of the National Association of Secretaries of State (NASS), the President of the National Association of State Election Directors (NASED), and a local election official chosen from among Election Center/International Association of Government Officials (iGo) by the local election officials on the GCC.

## Election Infrastructure Subsector Coordinating Council

In February 2018, the Election Infrastructure Subsector Coordinating Council (EI SCC) was established following adoption of an operating charter. Like all SCCs, the EI SCC is self-governing, enabling private-sector critical infrastructure owners and operators and industry representatives to work jointly on Subsector-specific strategies, policies, and activities. The SCC was chartered with 24 organizations, representing the spectrum of organizations involved in Subsector operations, with future changes in membership possible to maintain its accurate representation of the EIS. The SCC will collaborate with the GCC and DHS as the SSA to address critical infrastructure security and resilience policies and efforts for election infrastructure.

## EI SCC Executive Committee

Similar to the EIS GCC, the EI SCC maintains an executive committee to guide the work of the EI SCC and coordinate with leadership counterparts from the EIS GCC.

## Working Groups

The GCC and SCC will leverage working groups of Subsector members to pursue specific initiatives. Through the Critical Infrastructure Partnership Advisory Council (CIPAC), the councils are able to form joint working groups made up of GCC and SCC members as well as subject matter experts. The GCC formed a Strategic Communications Working Group to establish information sharing procedures and protocols. A working group was also formed to draft the SSP. The EIS will use this working group structure to pursue the goals and objectives outlined in the SSP.

## Value Proposition for Participation in the Sector Partnership

Election agencies recognize the importance of partnerships and continually make them a cornerstone of their programs. Partnerships provide subject matter experts, training programs, educational opportunities, and information-sharing mechanisms. As the Subsector redoubles efforts to address challenges posed by diverse technologies, evolving threats, and a spectrum of vulnerabilities across jurisdictions, the EIS partnership structure builds on the traditions of using partnership by providing:

Information exchange with the Federal Government and Subsector stakeholders, including development, validation, and sharing of best practices;

- Improved access to actionable, timely, and accurate threat information;
- Access to and influence in the development of exercises, training, tools, and resources to meet evolving operating conditions; and
- Inclusive processes for understanding and addressing vulnerabilities.
- Participating in the public-private partnership improves partners' situational awareness and understanding of Subsector risks, enabling members to more effectively:
- Minimize disruptions and improve resilience to ensure free, fair, and secure elections; and
- Raise public recognition for preparedness, continuity, and proactive management of election system risks to maintain and enhance confidence in election systems.

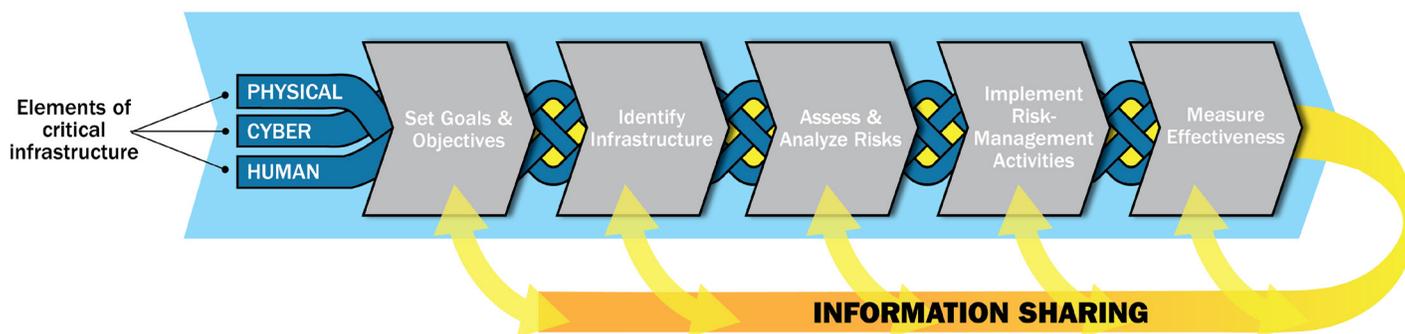
# 3 ELECTION INFRASTRUCTURE RISK MANAGEMENT

This chapter provides an overview of risk management for critical infrastructure and how it is applied in the EIS to promote the security and resilience of elections. More detailed information is provided in Appendix C.

## 3.1 Risk Management

The critical infrastructure risk management framework provides a common rubric for all stakeholders in the EIS to manage risks in their unique operating environments by setting goals and objectives; identifying their election infrastructure; assessing and analyzing risks to their infrastructure; and implementing management actions.

Figure 2. Critical Infrastructure Risk Management Framework



- **Identify Infrastructure:** EIS infrastructure exists at the federal, state, and local levels; is owned by the government and the private sector; and includes human, physical, and digital/cyber assets, networks, and systems. Specific infrastructure may be unique to a given jurisdiction, but there are commonalities across all jurisdictions as discussed in Section 2.1.
- **Assess and Analyze Risks:** Risk assessments examine the vulnerabilities, threats, and consequences to ascertain and analyze risks to help officials prioritize management strategies. Risk assessments completed at the state and local level should be documentable, reproducible and defensible.
- **Implement Risk Management Activities:** The Subsector has numerous, diverse risk environments which require election officials to prioritize their risk management activities to address their specific risk environments.

In considering the risks to election infrastructure, the EIS is especially aware of cyber risks, which various capabilities, threats, and intentions. Although the EIS already employs substantial security capabilities to mitigate cyber risks, increasing use and dependence on technology is expanding the EIS risk profile. DHS provides capabilities to support EIS management of cyber risks and the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*<sup>13</sup> provides standards, guidelines, and practices that can be applied to election risk management.

## 3.2 Bolstering Risk Management Capabilities

Information sharing, training and exercises, and leveraging R&D capabilities are three important strategies to advance the EIS's risk management capabilities.

### Information Sharing

Information sharing underlies every component of the risk management framework and is a tool to improve planning for and response to incidents. Secure access portals, newsletters, fusion centers, and other capabilities link levels of government

<sup>13</sup> National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

and EIS stakeholders. At the federal level, the EIS SSA operates the Homeland Security Information Network – Election Infrastructure Subsector (HSIN-EIS) portal, which provides a platform to share For Official Use Only (FOUO) information with EIS stakeholders. The EIS SSA is also working to provide clearances to election officials and SCC members through the Private Sector Clearance Program.

At the state and local level, fusion centers provide ties between infrastructure stakeholders and the law enforcement community, while organizations such as NASS and NASED disseminate information through nearly continuous communication to election officials.

Finally, the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) develops reporting in concert with DHS and other Subsector stakeholders to keep the EIS up-to-date on intelligence, best practices, mitigation strategies, and other valuable information for situational awareness.

## Training and Exercises

Training from national election organizations offers a level playing field for election officials across the Nation, providing consistency in an area otherwise marked by variance in approaches and requirements. These trainings are supplemented by federally provided curricula, such as DHS's [Federal Virtual Training Environment](#) which focuses on cybersecurity, and the [Federal Emergency Management Agency \(FEMA\) Emergency Management Institute](#) independent study courses on preparedness and response.

The EIS is committed to developing and delivering training to Subsector partners to meet their needs. Trainings are supplemented by tabletop exercises, which include engagements with government and private sector partners. Scenarios enable the Subsector to examine potential incidents before they occur, focusing on threats or vulnerabilities specific to the needs of the various jurisdictions.

## Research and Development

R&D enables better management of risk through development of new technologies based on stakeholder requirements. The EIS and SSA will work to formalize R&D plans and processes at the federal level to bring new knowledge, techniques, and capabilities to the Subsector.

# 4 VISION, MISSION, GOALS, AND PRIORITIES

## ELECTION INFRASTRUCTURE SUBSECTOR GCC VISION

Provide a unified government approach to enhance security and resilience efforts to ensure secure elections.

## ELECTION INFRASTRUCTURE SUBSECTOR GCC MISSION

Coordinate and advocate state and local election administration perspectives and needs across the spectrum of infrastructure service providers, governmental partners, funders, supporters, and other stakeholders.

This chapter outlines the EIS GCC’s Goals and Objectives for how best to support the Subsector’s continuing effort to secure the essential belief that Americans have trust in their elections. This is done by increasing awareness internally and externally, providing direct support to administrators, and securing the necessary short-, medium-, and long-term investments. The goals provide a framework to guide resilience efforts and improve EIS risk management practices.

Table 1. Chemical Sector Goals and Priorities

Goals	Priorities
<div style="text-align: center;">  <p><b>INFORMATION SHARING</b></p> <p>Ensure timely information sharing and consumption throughout the Subsector to promote clear information about security threats, probabilities, vulnerabilities, controls and responses.</p> </div>	<ol style="list-style-type: none"> <li>1. Implement an information-sharing environment that ensures the availability and flow of accurate, timely, and relevant Subsector information, intelligence, and incident reporting.               <ol style="list-style-type: none"> <li>a. Identify and maintain proper points of contact (POC) for state and local officials.</li> <li>b. Harmonize terms and vernacular for the EIS to ensure consistency of messaging and communication.</li> </ol> </li> <li>2. Utilize a digital network that links all state and local election officials with each other and with GCC-approved support organizations, services and products.               <ol style="list-style-type: none"> <li>a. Enhance the ability of state election officials to effectively assist with the protection of critical infrastructure inside their jurisdictions whether within or out of their control.</li> <li>b. Ensure that the benefits of the critical infrastructure designation be realized by local election officials, regardless of the level of engagement or capacity of their respective state election officials.</li> </ol> </li> <li>3. Employ a strategic communications effort to ensure that the election profession is able to define, inform, shape or otherwise participate in the public narrative around elections security in America.               <ol style="list-style-type: none"> <li>a. The EIS GCC Executive Committee, on behalf of the Council and industry, may craft messaging, where appropriate, that supports the general posture: the election profession is actively engaging on security and acting to protect the infrastructure.</li> </ol> </li> </ol>



### INCREASING CAPACITY

Support efforts that will increase election officials' capacity to defend against, detect, and recover from security incidents; and ensure a common understanding and approach to building resilience.

1. Continually review and modify, as needed, the Subsector's objectives, risk environments, priorities, mitigations, and available resources.
2. Educate state and local election officials regarding cybersecurity services and resources available from DHS, EAC, Multi-State Information Sharing and Analysis Center (MS-ISAC), and other public and private institutions.
3. Coordinate and extend the benefits of extra-governmental election security efforts to all election officials and to develop a common understanding of the Subsector.
4. Develop a set of technical, communications, operational continuity, and incident response plan templates.
5. Develop, maintain, and measure training for all election officials.
6. Support state-based efforts to help local election officials defend, detect, and recover from incidents.
7. Partner with the SCC to facilitate election security improvements across the election supply chain.



### RESOURCES

Work to establish consistent sources of funding that are appropriately flexible to support the Subsector's cyber resilience and national security efforts.

1. Work as a Council to identify election infrastructure security and resource gaps.
2. Work with partners to identify funding needed to fill those gaps.
3. Provide a forum to discuss election policy.

# 5 SUBSECTOR ACTIVITIES AND MEASURING EFFECTIVENESS

This chapter outlines the activities that the Subsector plans to complete in the short-, medium-, and long-term to meet the goals and priorities outlined in Chapter 4. The activities below are organized by Information Sharing, Capacity Building, and Financial Resourcing to align with the Goals and Objectives. The table below also assigns threshold priorities and measures of success for each activity, serving as metrics to allow for initial measurement of Subsector activities as the EIS partnership continues to mature.

As the EIS partnership deepens, the Subsector will continue to explore how to best quantify voluntary partnership activities' contribution to risk reduction and enhanced resilience across the election infrastructure landscape. This will include contributing to the existing DHS performance metrics system, which tracks the progress of Council activities across the critical infrastructure partnership framework. This effort to assess effectiveness of Subsector efforts should not preclude or impinge upon the measurement efforts of individual EIS partners.

Table 2. Election Infrastructure Subsector Priorities, Activities, and Measures of Success

GOAL MAP	PRIORITY	ELECTION SUBSECTOR ACTIVITY	MEASURES OF SUCCESS
	Short	Finalize and adopt Version 1 of the Information Sharing Protocols (ISP)	Final draft and vote of GCC
	Short	Distribute Version of the ISP to all election officials	Number of election officials who acknowledge receipt
	Medium	Identify all state, local, and territorial election points of contact	Number of state, local, and territorial election officials in the contact list
	Short	Finalize and adopt glossary of election and cyber terms	Publication after approval vote of GCC and disbursement with receipt confirmation by election officials
	Medium	Finalize and adopt an Election Infrastructure Operational Environment and Known Risk Profile	Publication after approval vote of GCC and disbursement with receipt confirmation by election officials
	Short	Design and adopt Digital Communication Portal (DCP) capable of reaching all election officials to enhance communications and support efforts from the federal level down, from the state level down, and from the local level up.	Final draft and approval vote of GCC
	Medium	Build and refine the DCP	DCP Version 1 released and kept current
	Long	Go live with the DCP	Number of election officials engaged
	Immediate	Develop and refine an outward facing strategic communications plan	Final draft and vote of GCC
	Immediate	Play an active role in shaping the public narrative around election security	Number of engagements between DHS Public Affairs and GCC Strategic Communications Working Group

GOAL MAP	PRIORITY	ELECTION SUBSECTOR ACTIVITY	MEASURES OF SUCCESS
	Short	Deploy an online training environment for election officials	Deployment after vote of GCC
	Long	Develop and deploy online training tools for election officials	Number of training tools deployed
	Short	Inventory and adopt as approved any materials that would be valuable for election officials	Publication of an Election Support Materials and Resources (ESMR) Guide
	Long	Ensure Distribution of approved ESMR Guide	Publication after vote of GCC and disbursement with receipt confirmation by election officials
	Long	Ensure election officials are utilizing available ESMR Guide	Download numbers and or certifications from DCP
	Medium	Identify resourcing gaps at the state level	Publication of a document describing state-level resourcing gaps
	Medium	Identify resourcing gaps at the local level	Publication of a document describing local-level resourcing gaps
	Medium	Identify the funding requirements necessary to fill gaps	Publication of a document with funding recommendations

# APPENDIX A. GOVERNMENT COORDINATING COUNCIL MEMBER PROFILES

This appendix lists the current organizations participating in the Election Infrastructure Subsector Government Coordinating Council (EIS GCC). The list will be updated as new members join the Council to reflect the full representation of the EIS.

## International Association of Government Officials (iGO)

The iGO has a very large contingent of election officials from around the Nation and world. The Domestic Election Section of iGO is committed to the idea of security election from the current threats. Three members on the GCC represent the iGO, though other GCC members may also be iGO members. The association aims to provide professional training and leadership development, through the promotion of networking, technology innovations, educational programs and legislative monitoring on national issues that affect county recorders, election officials, treasurers, and clerks, to better serve the public.<sup>14</sup>

## National Association of Secretaries of State (NASS)

In 40 states, the Secretary of State serves as the chief election official, charged with driving state election policy and ensuring compliance with the rules. NASS has eight members on the GCC. Founded in 1904, the NASS is the Nation's oldest, non-partisan professional organization for public officials. Membership is open to the 50 states, the District of Columbia, and all U.S. Territories. NASS serves as a medium for the exchange of information between states and fosters cooperation in the development of public policy. The association has key initiatives in the areas of elections and voting, state business services, and state heritage/archives.<sup>15</sup>

## National Association of State Election Directors (NASED)

The NASED mission is to promote accessible, accurate, and transparent elections in the United States and U.S. Territories. NASED has six positions on the GCC. NASED was formed in 1989 when a group of state election directors and administrators met in Reno, Nevada. The driving issue at that time that spurred the group to organize was the concern that national networks were releasing presidential election results before all polls had closed. HAVA has increased the importance for communication and coordination among state election directors. Though the issues have changed somewhat over the years, the purpose of NASED has remained the same—to serve as an exchange of best practices and ideas.<sup>16</sup>

## National Association of Election Officials

The National Association of Election Officials, also known as the Election Center, is a non-profit organization built to promote, preserve, and improve democracy. The Election Center may appoint three local election officials to the GCC. Its members are almost exclusively government employees whose profession it is to serve in voter registration and elections administration. This includes voter registrars, elections supervisors, elections directors, city clerks or city secretaries, county clerks, county recorders, state legislative staff, state election directors and the Secretary of State for each of the individual states, territories, and the District of Columbia. The Election Center provides its members with an alert service, which informs and updates state, city, and other elections and voter registration officials regarding legislation, regulations, court decisions, and Justice Department rulings that affect the conduct of voter registration or elections administration. Additionally, the Election Center performs research for such governmental units concerning the similarities and differences in state or local laws, regulations, or practices concerning voter registration and elections administration.<sup>17</sup>

<sup>14</sup> International Association of Government Officials (iGO), "About iGO," accessed May 11, 2018, <https://iaogo.org/about/>.

<sup>15</sup> National Association of Secretaries of State (NASS), "About NASS," accessed May 11, 2018, <http://www.nass.org/index.php/about-nass>.

<sup>16</sup> National Association of State Election Directors (NASED), "About NASED's History," accessed May 11, 2018, <https://www.nased.org/about-nased/>.

<sup>17</sup> National Association of Election Officials—Election Center, "About Us," accessed July 18, 2018, <https://www.electioncenter.org/about-us.html>.

## U.S. Department of Homeland Security (DHS)

As the designated SSA for the EIS, DHS's primary role is to build trusted partnerships and advance a national unity of effort to strengthen and maintain secure, functioning, and resilient election infrastructure, as laid out in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). DHS performs this role (as well as a similar role for other critical infrastructure sectors) via the National Protection and Programs Directorate (NPPD), which encompasses a variety of personnel, capabilities, resources, and technical expertise that state and local election officials can leverage on a voluntary basis to support the security and resilience of their election infrastructure. Under PPD-21 and the NIPP, DHS provides a venue for a voluntary, structured partnership approach between the government and the private sector for protection, security, and resilience of critical infrastructure. The EIS GCC and SCC are established under this framework.<sup>18</sup>

## U.S. Election Assistance Commission (EAC)

As the primary partner in the sector for the DHS, the EAC brings election official support and management experience to the table as this new sector stands up. The EAC was established by HAVA. EAC is an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. EAC also accredits testing laboratories and certifies voting systems, and audits the use of HAVA funds. Other responsibilities include maintaining the national mail voter registration form developed in accordance with NVRA. HAVA established the Standards Board and the Board of Advisors to advise EAC. The law also established the Technical Guidelines Development Committee to assist EAC in the development of voluntary voting system guidelines. The four EAC commissioners are appointed by the president and confirmed by the U.S. Senate. EAC is required to submit an annual report to Congress as well as testify periodically about HAVA progress and related issues. The commission also holds public meetings and hearings to inform the public about its progress and activities.<sup>19</sup>

### EAC Board of Advisors

The EAC Board of Advisors is a 35-member board composed of representatives from the National Governors Association; National Conference of State Legislatures; NASS; NASED; National Association of Counties; iGO; Election Center; International Association of Clerks, Recorders, Election Officials, and Treasurers; U.S. Commission on Civil Rights; and Architectural and Transportation Barriers Compliance Board. Other members include representatives from the U.S. Department of Justice, Office of Public Integrity, and the Civil Rights Division; the director of the U.S. Department of Defense Federal Voting Assistance Program; four professionals from the field of science and technology, one each appointed by the Speaker and the Minority Leader of the U.S. House of Representatives, and the Majority and Minority leaders of the U.S. Senate; and eight members representing voter interests, with the chairs and the ranking minority members of the U.S. House of Representatives Committee on House Administration and the U.S. Senate Committee on Rules and Administration each appointing two members. Following the passage of HAVA, the National Association of County Recorders, Election Officials and Clerks and the International Association of Clerks, Recorders, Election Officials, and Treasurers merged to form the International Association of Government Officials. It advises the EAC through review of the voluntary voting systems guidelines (VVSG) described in HAVA. This includes review of the voluntary guidance and best practices recommendations therein. It functions solely as an advisory body under the provisions of the Federal Advisory Committee Act.<sup>20</sup>

### EAC Standards Board

The Standards Board is a 110-member body designated by HAVA to assist EAC in carrying out its mandates under the law. The board consists of 55 state election officials selected by their respective chief state election officials, and 55 local election officials selected through a process supervised by the chief state election officials. Similar to the EAC Board of Advisors, the Standards Board advises the EAC through review of the VVSG, voluntary guidance, and best practices under HAVA.<sup>21</sup>

<sup>18</sup> U.S. Department of Homeland Security (DHS), "About DHS," accessed May 11, 2018, <https://www.dhs.gov/about-dhs>.

<sup>19</sup> U.S. Election Assistance Commission (EAC), "About U.S. EAC," accessed May 11, 2018, <https://www.eac.gov/about-the-useac/>.

<sup>20</sup> U.S. Election Assistance Commission (EAC), "Advisory Boards: Board of Advisors," accessed May 11, 2018, <https://www.eac.gov/about/board-of-advisors/>.

<sup>21</sup> U.S. Election Assistance Commission (EAC), "Advisory Boards: Standards Board," accessed May 11, 2018, <https://www.eac.gov/about/standards-board/>.

# APPENDIX B. SUBSECTOR COORDINATING COUNCIL MEMBERS

This appendix lists the current organizations participating in the Election Infrastructure Subsector Coordinating Council (EISSCC).<sup>22</sup> The list will be updated as new members join the Council to reflect the full representation of the EIS.

ORGANIZATION	ORGANIZATION
Associated Press (AP)	MicroVote
BPro Inc.	PCC
Clear Ballot Group	Pro V&V
Crosscheck	Runbeck Election Services
Democracy Live	SCYTL
Democracy Works	SLI Compliance
Demtech Voting Solutions	Smartmatic
Dominion Voting Systems	Tenex Software Solutions, Inc.
Electec, Inc.	Unisyn Voting Solutions
Election Systems and Software (ES&S)	VOTEC
Electronic Registration Information Center (ERIC)	Votem
Everyone Counts	VR Systems
Hart Intercivic	
KNOWInk	

<sup>22</sup> U.S. Department of Homeland Security, "Government Facilities Sector – Election Infrastructure Subsector: Council Charters and Membership," accessed July 17, 2018, <https://www.dhs.gov/government-facilities-election-infrastructure-charters-and-membership>.

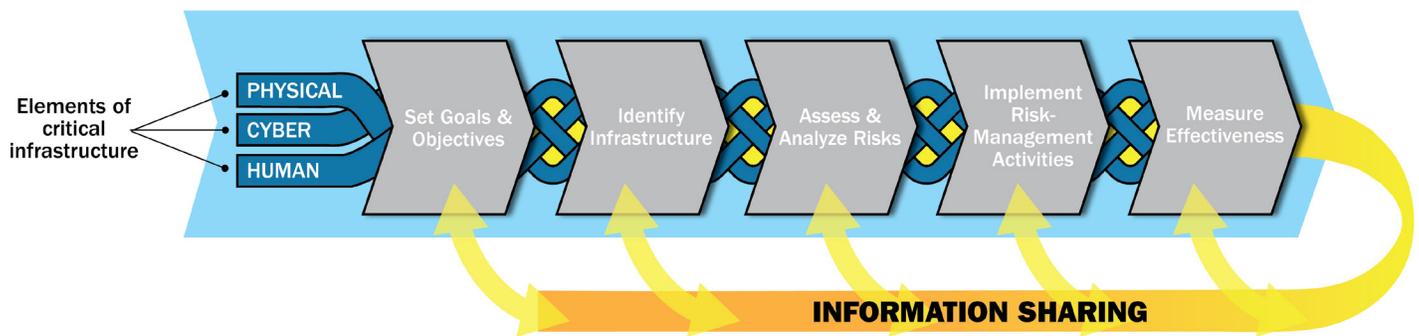
# APPENDIX C. RISK MANAGEMENT AND NATIONAL PREPAREDNESS

This appendix provides additional details to supplement the ongoing efforts and planned approaches that support risk management and the Subsector’s preparedness, response, and recovery following an incident that affects operations. The central focus of the Subsector’s goals and objectives is election security and resilience.

## Risk Management

Risk management activities are the foundation of critical infrastructure programs. Under the NIPP 2013 Risk Management Framework, risk is the potential for an adverse outcome from an event, determined by the event’s likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs. To systematically address these complexities, the EIS embraces the Risk Management Framework, which provides a common framework for election officials to identify their infrastructure; assess and analyze their risks; identify and prioritize risk management activities; and measure their effectiveness. The EIS goals and objectives discussed in this SSP are directly rooted in this risk management framework.

Figure 3. Critical Infrastructure Risk Management Framework



## Identify Infrastructure

Nationally, the EIS is characterized by distributed but inter-related systems with governance that varies state-to-state and jurisdiction-to-jurisdiction. Infrastructure criticality is viewed differently across jurisdictions and area of responsibility based on each partner’s unique situation, operating models, and associated risk.

SLTT governments represent the majority of the EIS and have the greatest understanding of the assets, systems, and networks that are crucial to their continued operations, the vulnerabilities inherent in a public-facing sector such as the EIS, and the available tools and services. The Subsector component categories described earlier—physical, digital/cyber, and human—can be used to ensure infrastructure is properly considered. This identification process needs to consider infrastructure assets operated by local jurisdictions, state governments, commercial partners, and federal agencies.

The Federal Government, election agencies, and private industry partners have personnel, processes, and tools to cooperatively identify critical local-, regional-, and state-level assets, systems, and networks critical to the EIS. These assets, systems, and networks include election-specific infrastructure and the infrastructure it is dependent on, such as electricity and IT. The different partners use the following:

- **SLTT Government Identification:** SLTT governments rely on existing internal structures to leverage the knowledge of EIS subject matter experts (SMEs) to support the identification of their election infrastructure assets.
- **Federal Capabilities:** SLTT entities and other Subsector partners leverage the expertise of Federal Government partners to work together to build and update inventories of assets significant at various government levels. Federal capabilities include the EAC; DHS’s Protective Security Advisors (PSAs) and Cybersecurity Advisors (CSAs), and critical infrastructure SSAs.

## Assess and Analyze Risk

Risk assessment is the cornerstone of the risk management framework, and election systems leverage numerous assessment methodologies to implement the framework. Although national-level assessments, such as the Strategic National Risk Assessment, are crucial to the comprehensive understanding of national risk, the EIS primarily conducts risk assessments at the state and local level focusing on vulnerabilities, assets, and capabilities to prioritize risk management activities and guide resource, budget, and policy decisions. All assessments conducted by the EIS should adhere to risk assessment methodology guidelines that ensure assessments are documented, reproducible, and defensible.

Election officials conduct a variety of assessments depending on the threat environment and are increasingly expected to provide options to increase the security posture of election facilities. Assessments can range from comprehensive (e.g., inclusive of threat, vulnerability, consequence, and dependencies) to those focused on a specific purpose (e.g., threat). Assessments completed within the EIS are used by the Subsector as an ideal starting point for assessing risk in terms of threats, vulnerabilities, and consequences.

**Assess Vulnerabilities** – A vulnerability is defined as the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Election officials have access to a variety of assessment tools from DHS and other EIS partners to collect, process, and analyze facility assessment data. The collected data can be used to develop metrics, conduct sector-by-sector and cross-sector vulnerability comparisons, identify security gaps and trends both within the EIS and across critical infrastructure sectors and subsectors. The data can also be used to establish Subsector baseline security survey scores, and track progress toward improving critical infrastructure security through DHS IP's programs, outreach efforts, and training.

**Assess Threats** – A threat is defined as the natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. When assessing risks to the election infrastructure, the threat of an intentional hazard is estimated as the likelihood of an attack that accounts for both the intent and capability of the adversary.

In assessing threats, the EIS considers the full spectrum of intentional and unintentional threat sources, including natural threats (e.g., hurricane, fire, and floods), man-made threats (e.g., chemical, radiological, and biological attacks), workforce threats (e.g., pandemic flu, insider threat, and human error), and cyber-related threats (e.g., technological hazard and degradation). Within the EIS, the assessment of natural threats is more defined based on experience and availability of historical data. Man-made threat sources are more complex. In the assessment of terrorist threats, the EIS considers both capability and intent as discrete subcomponents of threats. The NIPP 2013 defines threat capability as the availability or the ease of use of tools or methods that could potentially be used to damage, disrupt, or destroy critical functions.

The EIS analyzes all types of applicable, potential threats and determines those of national and local significance for inclusion within the threat portion of the Subsector's risk assessment. Threat assessments are most effective when applied to a specific elections threat source in a specific geographic region, state, or locality. The EIS leverages several threat assessments:

- **SLTT Fusion Center Threat Assessments** – Subsector partners leverage fusion center and law enforcement-generated threat assessments and analyses. Fusion centers combine real-time threats with risk information, such as historical risk, in a timely manner; thus, enabling the EIS to effectively manage their security posture.

### Identification of infrastructure assets and systems can happen at several levels:

**LOCAL JURISDICTIONS** – Local jurisdictions including counties, cities, and parishes conduct elections throughout the Nation. They coordinate with various organizations, contractors, and with their state governments to carry out the elections, but every local jurisdiction is involved in elections throughout the Nation.

**STATE GOVERNMENTS** – State governments are involved in the elections process throughout the Nation. Their involvement varies by state, but they all have some part in utilizing critical assets to conduct elections.

**PARTNERS** – Various contractors are utilized at varying levels of degree. Contractors often have critical components in the operation of elections that are required for the continuity of the elections. Examples of these components include voting technology providers and ballot printers.

**FEDERAL AGENCIES** – The U.S. Postal Service (USPS), in particular, is a Federal agency that provides a critical component for voter participation. In some jurisdictions, all voting is conducted through the mail.

- **Federal Threat Assessments** – The EIS also utilizes threat sources and analysis from the Federal Government, including the Office of Cyber and Infrastructure Analysis (OCIA), the DHS Office of Intelligence and Analysis (I&A), and the Federal Bureau of Investigation (FBI). Information-sharing portals, such as DHS’s HSIN-EIS and the FBI’s Guardian Program, are leveraged by EIS partners as mechanisms to share threat-related information.

**Assess Consequences** – A consequence is defined as the effect of an event, incident, or occurrence that reflects the level, duration, and nature of the loss resulting from the incident. An elections-related physical or cyber event would result in political, psychological, and governance consequences. The assessment of consequences is crucial to the risk management decision-making process. The EIS community recognizes that consequences may include:

- **Political** – Refers to the government or public affairs of the Nation, which includes those public offices affected by an election failure, as well as the confidence that the Nation has in the results of other, unaffected election outcomes.
- **Psychological** – Refers to the effect on morale and confidence in national economic and political institutions, including changes in perceptions emerging after a significant incident that affects individuals’ sense of safety and well-being and may result in aberrant behavior.
- **Governance** – Refers to the effect on the government or industry’s ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out national security-related missions. This element is measured in an increased response time or in the decreased abilities of surrounding capability elements to respond. Mission impact will have some degree of cascading effect to other sectors.

## Implement Risk Management Activities

The risk that each component (vulnerability, threat, and consequence) could have an election-related activity and the relative importance of existing risk management gaps help to determine the prioritization of protective initiatives. To ensure that resources are applied in areas that will best mitigate these risks, election infrastructure and associated security and resilience programs must be prioritized based on risk.

However, risks are multidimensional. A less high-profile election system may be exposed to a greater risk necessitating a deprioritized response in comparison to a vital election system that faces a lesser but catastrophic risk. Affordability, return on investment, and sustainability are key considerations in determining which resource shortfalls will be addressed immediately or over time. Systematic methods for assessing the Subsector’s assets, systems, and networks provide data to inform budget and resource allocations. Each EIS process may prioritize risk management activities based on system usage, along with activity costs, potential for risk reduction, and varying levels of infrastructure criticality—shaped by different views across jurisdictions and areas of responsibility. For instance, in states where the voter registration system is not actively consulted or updated on Election Day, the need for urgent resilience on that day is less important than in jurisdictions with same day registration or live voter updates on Election Day.

### Information Sharing Initiatives

Information sharing is critical, especially during incidents of national significance or affecting multiple election jurisdictions simultaneously or in real time. Information-sharing initiatives are crucial to ensuring information flows across all levels and the private sector, as appropriate. Information-sharing initiatives are augmented by the HSIN-EIS, websites, professional associations, and conference presentations. The GCC and SCC conduct regularly scheduled meetings and conference calls to discuss security and resilience programs and strategies affecting a specific discipline or the EIS as a whole.

Information sharing underlies all components of the risk management framework, facilitates collaborative problem solving, and is critical to a common operating picture, particularly during expanding incidents or incidents that affect multiple jurisdictions simultaneously. Information-sharing mechanisms used by SLTT agencies to share information with public and private sector partners include:

- **Secure Access Portals:** SLTT agencies use HSIN portals and TRIPwire<sup>23</sup> (Technical Resource for Incident Prevention) to receive key analysis and to collect, analyze, and disseminate information to vetted partners. Agencies may also utilize other federal resources, such as the FBI Guardian system.
- **Bulletins and Newsletters:** These information products include regular EIS-specific or topical open-source reports; newsletters containing upcoming projects, best practices, or achievements; and bulletins or reports forwarded from other entities.

<sup>23</sup> U.S. Department of Homeland Security (DHS), “Technical Resource for Incident Protection (TRIPwire),” accessed May 8, 2018, [https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?\\_nfpb=true&\\_pageLabel=LOGIN](https://tripwire.dhs.gov/IED/appmanager/IEDPortal/IEDDesktop?_nfpb=true&_pageLabel=LOGIN).

- **Briefings:** SLTT agencies regularly conduct briefings to inform their leadership of program activity, improvement, and strategy; disseminate information with various sectors; share best practices; and communicate threat information and adversary tactics. Briefings are conducted in-person, on conference calls and webinars, or during conferences (e.g., NASS conferences, NASED conferences, local election official association conferences).
- **Fusion Centers:** Many SLTT critical infrastructure programs are integrated with SLTT fusion centers and have strong engagement with fusion centers on activities with a critical infrastructure nexus. Fusion centers deliver wide-ranging intelligence products (e.g., joint intelligence products); provide an accessible hub to homeland security activity and partnerships (i.e., DHS, FBI, or fusion liaison programs); and offer resources to improve homeland security capabilities such as trainings, webinars, or toolkits.
- **Conferences:** SLTT agencies host and attend conferences to share best practices, promote threat and hazard awareness, achieve critical infrastructure activity situational awareness, and network with subject matter experts and the critical infrastructure community. Conferences also provide educational opportunities for critical topics, such as cybersecurity.
- **Partnerships:** Public-private partnership organizations (e.g., InfraGard<sup>24</sup>); government and private sector councils, working groups, and task forces; Information Sharing and Analysis Centers (ISAC); academic institutions; and interagency relationships provide unique opportunities for two-way information sharing on hazards, threats, Subsector interdependencies, and best practices.

## Federal Information Sharing

The SSA utilizes a variety of mechanisms to disseminate information to EIS stakeholders, such as CIPAC conference calls, coordinating information calls with federal partners responding to incidents, and posting information to the HSIN-EIS portal. By ensuring information is readily available and easily accessible, HSIN-EIS provides a valuable method to share up-to-date FOUO and incident information with SCC members and Subsector stakeholders. DHS's Private Sector Clearance Program sponsors security clearances for GCC members, election officials, and SCC stakeholders to enable the sharing of classified information

## SLTT Information Sharing

Information sharing at the SLTT level incorporates federal information-sharing mechanisms with daily coordination conducted primarily through SLTT fusion centers, many of which co-locate with SLTT critical infrastructure programs and law enforcement agencies. This proximity results in strong partnerships and close collaboration at the SLTT level. In addition, the NASS and the NASED have robust, nearly continuous communications with their member states on various issues related to EIS security. State election officials regularly distribute relevant information to local elections jurisdictions. As a result, the intersection of NASS, NASED, and their connection to the local election offices provides a reasonable avenue for information dissemination as do national and state-level membership organizations for local election officials. Public-facing SLTT agency websites are also relied upon heavily to share with the public.

## Election Infrastructure Information Sharing and Analysis Center

The MS-ISAC is a voluntary and collaborative effort designated by DHS as a key information sharing resource for SLTT governments. It provides a variety of services and capabilities such as real-time network monitoring; threat and vulnerability monitoring; incident response and remediation; strategic, tactical, and operational intelligence; training sessions and webinars; and promoting security best practices.

In partnership with DHS, the EIS established an EI-ISAC under the MS-ISAC to facilitate the sharing of cyber and/or critical election data among all state and local election officials, their employees, and others as appropriate. Through member sharing and coordination with partners such as the National Cybersecurity and Communications Integration Center (NCCIC) and industry partners, the EI-ISAC correlates and organizes information and collaborates with partners to develop joint reports on threat intelligence, best practices, and mitigation strategies. This provides broad situational awareness to keep the EIS informed and prepared.

## Election Security Training and Exercises

Existing state and local training for election administrators and partners vary depending on jurisdiction. For example, many jurisdictions require mandatory courses and some offer certifications, but others are member-run with loose curricula and limited resources. Training from national election organizations and the Federal Government offers a consistent baseline

<sup>24</sup> InfraGard, "Welcome to InfraGard," accessed May 8, 2018, <https://www.infragard.org/>.

to improve the capabilities of public and private sector EIS stakeholders. Topics include active shooter incident response, critical infrastructure security and resilience, best practices for administering elections, and cybersecurity. Training platforms include FEMA's Emergency Management Institute and NPPD's Federal Virtual Training Environment (FedVTE), which offers cybersecurity training ranging from beginner to advanced levels, including elections-specific courses currently in development.

The delivery and continued development of effective training and exercises is critical to risk management. To ensure the coordinated development and delivery of training and exercises, the EIS relies on the following strategies:

- Capture, report, and prioritize needs of Subsector partners.
- Examine and leverage current federal, state, and local programs for use in the EIS.
- Leverage a network of Subsector members and partners to best serve sector partners and reach each of the nearly 9,000 election jurisdictions operating in the United States.
- Partner with academia and other experts to inform critical infrastructure-related curricula, and educate and train election administrators and operational support, including IT professionals who provide election services.

Finally, the EIS will use tabletop exercises to drill into the Subsector's response to risks, which includes engagement with private sector election partners.

## Managing Cyber Risks

The EIS and election administrators across government, including states, territories, and nearly 9,000 election jurisdictions, face cyber threats from criminals, hackers, terrorists, and nation-states with varying degrees of capability and intention to attack elections. The EIS's existing security capabilities are substantial and often mitigate cyber threats to voting systems because most are not connected to the Internet. Other election systems, however, have substantial digital/cyber components and, overall, the Subsector's increasing dependence on technology could increase vulnerability to exploitation.

The EIS collaborates with the DHS Office of Cybersecurity and Communications (CS&C) to conduct cybersecurity assessments, enhance cybersecurity implementation through Cyber Resilience Reviews, and promote and develop cyber risk management strategies and partnerships through the DHS critical infrastructure cybersecurity program. The EIS's collaborative approach to cyber information sharing and cybersecurity is supported by HSIN-EIS and working groups responsible for information sharing and cybersecurity. Cyber-related alerts and resilience strategies are disseminated throughout the sector through the MS-ISAC, EI-ISAC and the U.S. Computer Emergency Readiness Team (US-CERT).

### National Institute of Standards and Technology Cybersecurity Framework

In response to Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636),<sup>25</sup> NIST developed a Framework for Improving Critical Infrastructure Cybersecurity,<sup>26</sup> in addition to a companion roadmap. The framework consists of standards, guidelines, and practices (including public-private coordination through the Critical Infrastructure Cyber Community Voluntary Program) that can be applied to elections to assist administrators and providers in managing cyber-related risk in election systems. The EIS will review the standards recommended by such bodies as NIST for possible recommendations when considering additional cybersecurity policies and procedures.

## Mitigating Disruptions from the Loss of Lifeline Functions

All critical infrastructure sectors rely on the security and availability of certain lifeline functions that are essential to Subsector operations. The functions important to the EIS include aspects of Communications, IT, Energy, and Transportation sectors. In the event of utility or transportation disruption, many components of the EIS are able to operate in a degraded fashion and registration management and elections could still function despite of loss of services. Engaging in robust training and exercises expand the understanding of lifeline function disruption consequences and establish effective mitigation practices.

## Research and Development Priorities

R&D plays a critical role in enabling homeland security partners to develop knowledge and technologies that more effectively reduce risk. New and innovative technologies can enhance the resilience and security of the election process. The GCC will work to establish a comprehensive R&D approach supported at the federal level to identify and validate R&D requirements.

<sup>25</sup> The White House, Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, February 12, 2013, <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

<sup>26</sup> National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.

## Election Infrastructure Subsector National Preparedness Efforts

A major focus for the EIS is preparedness for cyber and physical disruptions in service either on Election Day or during important days on the election calendar. The EIS must be able to maintain jurisdictions' ability to deliver the election service continuously during important election periods. This means providing real-time or near real-time service to election information (e.g., the state voter registration system) even when regular delivery mechanisms have failed due to a natural disaster or security breach. EIS resilience also includes the ability to restore regular services after such events and the ability to continuously change or modify these delivery mechanisms, if needed, in the face of new risks. Backups, both physical and technological, and disaster recovery operations are part of the process of restoring delivery mechanisms.

Due to the importance of the EIS mission, the Subsector's security and resilience strategies and activities cross the entire national preparedness spectrum of prevention, protection, mitigation, response, and recovery from an incident. Efforts to enhance the national preparedness mission areas translate to a more secure and resilient EIS and, therefore, a more secure and resilient national psyche.

Numerous security and resilience programs and activities exist throughout the Subsector including measures designed to prevent, deter, and mitigate threats to election administration; reduce vulnerability to election mischief; minimize the consequences on election outcomes and perception; and enable timely, efficient response and restoration following incidents. Across the United States, the EIS security and resilience programs and activities are organized and executed to be consistent with the five national preparedness frameworks—National Prevention Framework, National Protection Framework, National Mitigation Framework, National Response Framework, and National Disaster Recovery Framework—in addition to the implementing the National Incident Management System. These programs and activities that contribute to the security and resilience of the Subsector are diverse and developed by numerous Federal and SLTT agencies, including NASS, NASED, the Election Assistance Commission (EAC), among others, along with EIS discipline-specific trade associations, and education and training institutions that support the Subsector's specialized capabilities. The EIS is charged with creating and maintaining security and resilience plans to support the five national preparedness mission areas—prevention, protection, mitigation, response, and recovery as they apply to the administration of elections.

### Prevention

Prevention efforts are closely related to efforts that address threats and are reflected in EIS activities to conduct assessments, such as threat assessments. EIS examples include:

- Provide timely, accurate, and actionable information and exchange information, data, and knowledge among federal, SLTT, and private sector EIS entities, as appropriate.
- Inform and direct cybersecurity preparedness efforts for the EIS, and other sectors by proxy.
- Perform regular software patching for all relevant systems to ensure vulnerabilities are addressed in a timely manner.
- Participate in information sharing activities to ensure cross sector information exchange.

### Protection

Protection efforts generally address vulnerabilities, such as in EIS programs and activities that focus on assessing vulnerabilities and addressing those vulnerabilities. Active shooter preparedness plans and other topics discussed in this plan are examples.

### Mitigation

Mitigation efforts transcend all three components of understanding critical infrastructure risk—threat, vulnerability, and consequence. Mitigation covers a wide range of activities that include anything from planning activities to long-term vulnerability reduction activities. EIS examples include:

Assess risk to enable decision-makers and EIS stakeholders to take informed action to reduce risk to the sector and increase their resilience.

Identify the threats and hazards that may affect the EIS, determine the frequency and magnitude of impact, and incorporate this into planning processes to make informed risk management decisions.

## Response

Response efforts are intimately tied to recovery efforts in that both help to minimize consequences. EIS examples include:

- Develop effective incident response playbooks and information sharing protocols.
- Develop detailed contingency plans to address potential incident ranging from natural disasters to cyber incidents.

## Recovery

Recovery efforts include those activities that are necessary to assist affected locations in recovering effectively from an incident. EIS examples include:

- Ensure communications among EIS, federal, and SLTT entities continue to support information sharing and documenting lessons learned.

# APPENDIX D. GLOSSARY OF TERMS

This appendix includes definitions of the terms used in the SSP and adapted from the NIPP. For a broader glossary of terms used by the EIS, please refer to the EAC's Glossary of Key Election Terminology.

## All Hazards

A term that encompasses threats or incidents, natural or man-made that warrant action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities.

## Consequence

The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with the economic impacts both direct and indirect and other negative outcomes to society.

## Critical Infrastructure

Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

## Critical Infrastructure Sectors

A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; PPD-21 identifies 16 critical infrastructure sectors.

## Election Systems

Includes infrastructure to manage voter registration, planning and execution of elections, counting and reporting of election results, and other software and hardware used by election officials.

## Federal Virtual Training Environment (FedVTE)

A free, online, and on-demand cybersecurity training system for federal/SLTT government personnel and veterans. Managed by DHS with support from the Department of Defense's Defense Information Systems Agency, FedVTE offers more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Courses range from beginner to advanced levels. Training is accessible from any Internet-enabled computer.

## Government Coordinating Council

Consists of representatives from across various levels of government (including federal and SLTT), as appropriate to the operating landscape of each individual sector, these councils enable inter-agency, intergovernmental, and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts.

## Homeland Security Information Network-Election Infrastructure Subsector

A trusted network to share Sensitive but Unclassified information with federal, state, local, territorial, international, and private sector partners.

## Lifeline Function

A function that is essential to the operation of most critical infrastructure sectors. The NIPP-2013 identifies communications, energy, transportation, and water as lifeline functions. Critical infrastructure partners should identify essential functions and resources that impact their businesses and communities.

## Private Sector Clearance Program

Program administered by the DHS designed to facilitate access to security clearances for private sector officials involved in the infrastructure protection mission.

## Risk

The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

## Sector Coordinating Council

Self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, which interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities. For the Election Infrastructure Subsector, the Council includes the owners and operators for the Subsector.

## Sector-Specific Agency

A federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

## Threat

A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

## Vulnerability

A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a give hazard.

# APPENDIX E. ACRONYMS AND ABBREVIATIONS

Table 4. Acronyms and Definitions

ACRONYM	DEFINITION	ACRONYM	DEFINITION
CIIA	Critical Infrastructure Information Act of 2002	ISAC	Information Sharing and Analysis Center
CIPAC	Critical Infrastructure Partnership Advisory Council	ISP	Information Sharing Protocol
CSA	Cybersecurity Advisor	IT	information technology
CS&C	Office of Cybersecurity and Communications	MS-ISAC	Multi-State Information Sharing and Analysis Center
DCP	Digital Communication Portal	NASED	National Association of State Election Directors
DHS	U.S. Department of Homeland Security	NASS	National Association of Secretaries of State
DRE	Direct Recording Electronic	NCCIC	National Cybersecurity and Communications Integration Center
EI	Election Infrastructure	NIPP 2013	National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience
EI-ISAC	Election Infrastructure Information Sharing and Analysis Center	NIST	National Institute of Standards and Technology
EIS	Election Infrastructure Subsector	NGO	non-governmental organization
EAC	Election Assistance Commission	NPPD	National Protection and Programs Directorate
EO 13636	Executive Order 13636: Improving Critical Infrastructure Cybersecurity	NVRA	National Voter Registration Act
ESMR	Election Support Materials and Resources	OCIA	DHS Office of Cyber and Infrastructure Analysis
FBI	Federal Bureau of Investigation	POC	Point of Contact
FedVTE	Federal Virtual Training Environment	PPD-21	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
FEMA	Federal Emergency Management Agency	PSA	Protective Security Advisor
FOUO	For Official Use Only	R&D	Research and Development
GCC	Government Coordinating Council	SCC	Subsector Coordinating Council
GIS	geographic information system	SLTT	State, local, tribal, and territorial
HAVA	Help America Vote Act	SME	Subject matter expert
HSIN-EIS	Homeland Security Information Network-Election Infrastructure Subsector	SSA	Sector-Specific Agency
I&A	DHS Office of Intelligence and Analysis	SSP	Subsector-Specific Plan
iGO	International Association of Government Officials	TRIPwire	Technical Resource for Incident
IP	Office of Infrastructure Protection		

ACRONYM	DEFINITION
TSBMD	Touch Screen Ballot Marking Devices
US-CERT	United States Computer Emergency Readiness Team
VSG	voluntary voting systems guidelines