ELECTION SECURITY NAVIGATORS

Program Guidebook

September 2023

Cybersecurity and Infrastructure Security Agency

Contents

EXECUTIVE SUMMARY 3

BACKGROUND 4

WHAT IS AN ELECTION SECURITY NAVIGATOR? 4

TYPES OF NAVIGATOR PROGRAMS 5

NAVIGATOR SUPPORT AND SERVICES 6

BUILDING AN ELECTION SECURITY NAVIGATOR PROGRAM 7

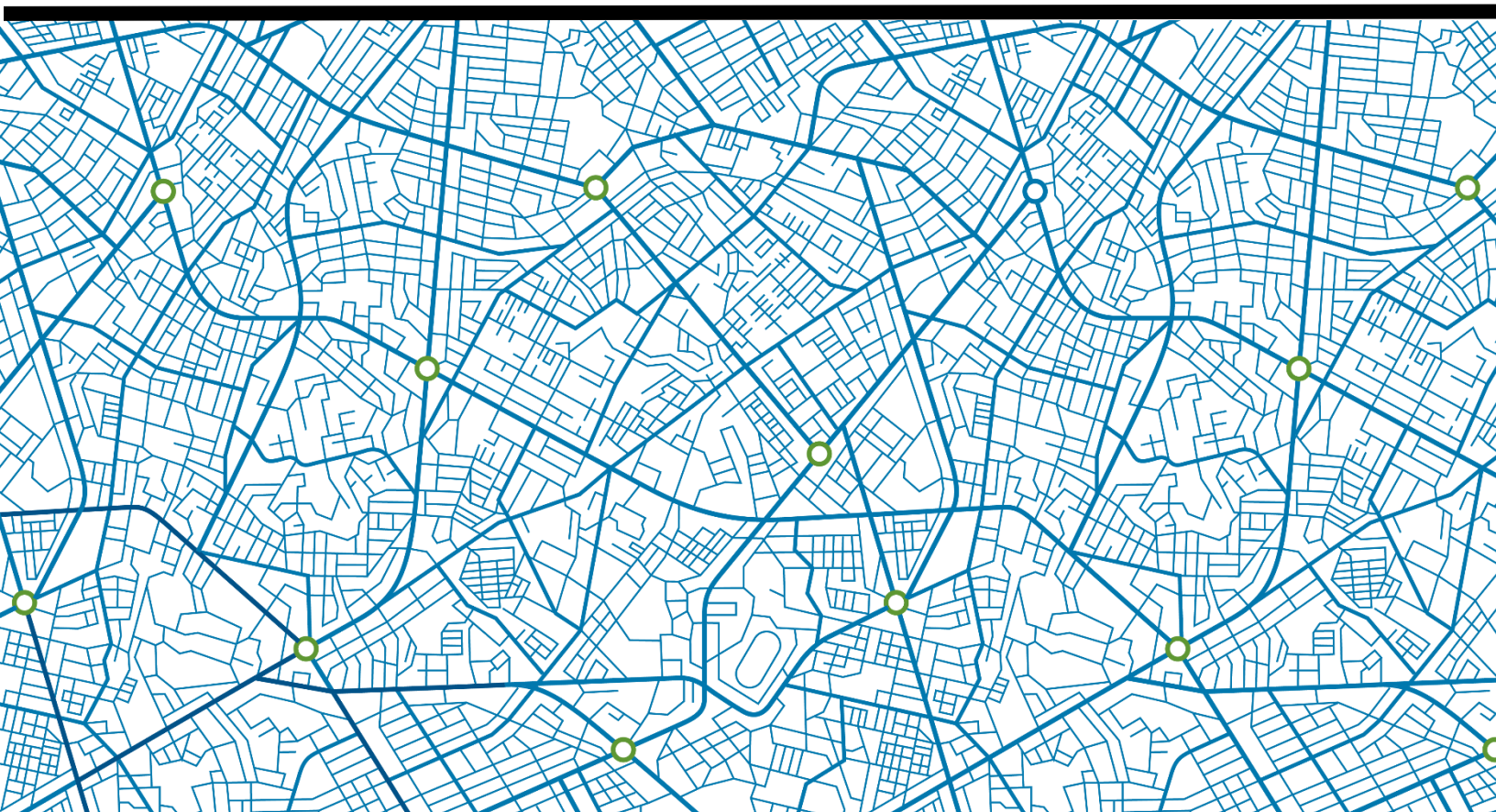
- Explore Authority and Administrative Oversight 7
- Identify Gaps Between Existing State Election Security Support and Local Needs 7
- Establishing a Program Baseline and Scope 7
- Identify Funding 8
- Choosing a Navigator 9
- Measuring Performance and Effectiveness 9

SHARING NAVIGATOR PROGRAM BEST PRACTICES 9

CONSIDERATIONS FOR IMPLEMENTING DIFFERENT NAVIGATOR PROGRAM MODELS 10

- Examples of Program Models 10
- Program Considerations 10

CONCLUSION 13



EXECUTIVE SUMMARY

Elections operate in a highly visible, yet resource-constrained environment, which poses ongoing challenges to ensuring security. Although state election offices and other state agencies have expanded election security support to local jurisdictions since 2016, resources and expertise remain limited. In some instances, resource limitations have driven competition and increased costs among jurisdictions. As a result, several states have developed programs for dedicated liaisons, known as "**navigators**," to reinforce or supplement election security efforts at both the local and state level.

Drawing on the experiences of states that have implemented navigator programs and similar efforts in recent years, this guidebook examines ongoing practices in this area and offers ideas for states that are considering adopting such a program or enhancing an existing one. Specifically, this guidebook outlines the roles, responsibilities, and capabilities of these programs, exploring the following topics:

- What is an Election Security Navigator?
- Navigator Support and Services
- Building a Navigator Program
- Sharing Navigator Program Best Practices

The concept of dedicated navigators for local election administrators is not new and has become a well-supported model across the election infrastructure subsector. Navigator programs are not "one size fits all," with each state developing its own unique approach. Some states may place emphasis on cybersecurity, while others may focus on broader election security risk management.

Navigator programs empower states to apply the expertise of a small group of personnel broadly, resulting in a force multiplier effect across jurisdictions. These programs can provide a wide range of support and services to local election offices. Varying by state, existing programs' support and services have included threat information sharing and analysis, training and exercises, risk assessments, mitigation guidance and implementation, incident response planning and reporting, and stakeholder engagement.

Establishing a navigator program is a multi-step process. These steps can include identifying funding and relevant authorities, assessing needs and gaps, defining program scope and scale, establishing a program baseline, leveraging partners, choosing a navigator and/or navigator team, and adopting a framework for monitoring and evaluating program performance.

Continued sharing of information and best practices among states with navigator programs and similar efforts can be useful during program development and implementation. For example, existing materials, such as baseline measurement tools or implementation plans, can be borrowed, customized, and repurposed. Through this guidebook and other activities, CISA will continue to seek opportunities to facilitate information sharing among navigators and across the broader election community.

Successful navigator programs have the potential to serve as critical force multipliers, supplementing limited resources on the local level to foster improved security and greater resilience in the Nation's election infrastructure.

BACKGROUND

U.S. elections are decentralized and administered at the state, local, and territorial level under jurisdictionally-specific legal and procedural frameworks, systems, and infrastructure. There is also wide variation in terms of resources, especially among small and medium-sized local jurisdictions that must often rely on constrained budgets and limited in-house expertise on cybersecurity and other emerging priority security issues. To help mitigate resourcing challenges, state election offices often support their local counterparts through information sharing, training, and management of shared infrastructure, such as statewide voter registration databases.

Following the 2016 elections, such support has been increasingly focused on cybersecurity and broader election security risk management. In several states, expanded support in this area has included the assignment of dedicated state liaisons, known in multiple states as "navigators," that help advance election security efforts down to the smallest jurisdiction.

WHAT IS AN ELECTION SECURITY NAVIGATOR?

An election security navigator (hereafter referred to as "navigator") is any liaison, regardless of title, assigned to reinforce or supplement local and state-wide election security efforts.

The title and organizational structure for navigator programs vary by state. While some states use the title of "navigator," other states use different terms. Navigators in most states are employed by the state election office, while others work for a different state agency or office, for example information technology and information security offices.

In practice, navigators may be involved in a wide variety of activities such as managing information sharing, offering onsite assistance, developing training, coordinating response efforts, and sharing actionable resources. The specific mission, role, and responsibilities of a navigator will vary by state. Ultimately, navigator programs can be developed to meet the needs of each election jurisdiction and tailored to reflect unique election operations and dependencies within each state.

Remember: *There is no "one size fits all" navigator program, but election security navigators can be vital resources for state and local officials and can address a variety of needs.*

TYPES OF NAVIGATOR PROGRAMS

Navigator programs may differ in terms of staffing, scope, and program mission. See *Table 1* for a few program models. For example, some states have employed as many as 10 dedicated navigators, while others utilize just one. Initially, states that were early adopters of navigator programs focused on supporting cybersecurity efforts to mitigate against cyber risk. Increasingly, depending on needs within their jurisdiction, navigators are supporting local election offices mitigating a wider spectrum of threats to election security, including physical risk, operational risk and countering foreign influence operations and disinformation.

Navigator programs can cover a wide range of election security issues, but most existing programs have coalesced around four main risk areas:

- Cyber Risk. Navigators focus on mitigating cyber risk through cybersecurity practices to protect networks, devices, and data from unauthorized or criminal use and protecting the confidentiality, integrity, and availability of information. In the context of elections, cybersecurity efforts focus on the networks, devices, and data used to administer elections, including election office websites, voter registration databases, voting equipment, and other systems, as well as the data stored in and managed by such systems.

- Physical Risk. Navigators help address physical risk through physical security efforts that include efforts to protect against unauthorized physical access of sensitive infrastructure and against acts of violence or other harmful activity targeting facilities, infrastructure, or personnel. In the context of elections, this can include the protection of election offices, storage and counting facilities, voting locations, ballot drop boxes, election workers, and voters themselves.

- Operational Risk. Operational risks are those that have the potential to impede the successful execution of operations. In elections, this includes any risk that could hinder the management of election operations, such as disruptions to the supply chain of ballot paper or availability of critical resources, such as electrical power.

- Foreign Influence Operations and Disinformation. Countering foreign influence operations and disinformation includes activities that build resilience to foreign malign actors' use of false information to undermine election infrastructure security. When targeting election infrastructure or voters, such efforts can sow discord and undermine confidence in election processes and results, often by amplifying incorrect or misleading information about elections, the voting process, or aspects of election technology and security.

NAVIGATOR SUPPORT AND SERVICES

Navigator programs can provide a wide range of support and services to local election offices, customized to align with the state's unique legal framework and infrastructure. Existing programs' support and services have included variations of the following items:

Navigator Support Area	Value to Election Officials
Information Sharing and Analysis	Evaluate, analyze, and share election security threat information (e.g., cybersecurity alerts) to ensure officials are receiving clear, concise, timely, and actionable information
Risk Assessment	Facilitate risk assessments that identify potential security gaps and vulnerabilities
Risk Analysis and Prioritization	Analyze risk assessments and data from technical service reports; recommend prioritization for mitigations
Mitigation Guidance	Recommend resources and technical services available to election officials that reduce risk and build resilience
Technical Implementation	Implement mitigation measures such as establishing operating procedures, initiating meetings with IT support, and drafting improvement plans
Incident Response Planning and Reporting	Update or develop customized incident response plans to ensure appropriate coordination and response between local, state, federal, and private sector partners; provide guidance on reporting requirements
Continuity of Operations Plan (COOP) Development	Update or develop customized plans to ensure continuity of operations during potential incidents
Training and Exercises	Provide elections officials with election security training or facilitate exercises and simulations to test incident response plans and procedures, and ensure overall operational readiness
Stakeholder Engagement	Raise awareness and build trust in election processes in local communities through stakeholder engagements
Template Development	Develop and use templates to standardize materials, such as standard operating procedures (SOPs), security checklists, or recovery plans

BUILDING AN ELECTION SECURITY NAVIGATOR PROGRAM

When state election officials begin building a navigator program, it is crucial to first consider the potential use cases, benefits, and whether the state can allocate adequate resources to effectively implement and manage the program. Such deliberations upfront can increase a program's success and long-term viability. Below outlines a few considerations to inform the initial planning process.

Explore Authority and Administrative Oversight

As jurisdictions work through initial planning, it is important to identify who has the authority or regulatory power to establish the program and who will assume the administration, risk, and costs of providing services. In some cases, like in Illinois,[1] legislation was necessary to establish the program. In other cases, such as Minnesota, legislation was not necessary.[2]

Identify Gaps Between Existing State Election Security Support and Local Needs

Identifying gaps between state election security support and services and the needs of local jurisdictions is a crucial step prior to crafting an implementation plan and can increase the likelihood of program success. For example, in a state where many local election offices lack or possess outdated incident response plans, the state may seek to create a navigator program with lines of effort that address incident response coordination, incident response plan development, and exercises that include incident response scenarios.

After conducting a needs assessment and customizing the program to benefit both the state and local jurisdictions, it may be helpful to begin researching existing models from states that have already deployed navigator programs. *Table 1* features examples of how some states and localities frame their programs.

Establishing a Program Baseline and Scope

Following the completion of the needs assessment, **organizations should seek to establish baseline metrics or indicators from which to measure progress against.** Resources such as CISA's Election Security Risk Profile Tool or Cross-Sector Cybersecurity Performance Goals Checklist may be helpful for developing benchmarks, which jurisdictions can customize based on their unique needs, infrastructure, and existing security posture.

Election security navigator programs inherently allow local election officials to tailor the program to fit their unique risk profiles and localized security needs. **The role of the navigator is to help identify those risks, assess areas for improvement, and, where appropriate, help create a plan of action to address them.** In scoping navigator programs, some states have focused primarily on cybersecurity, while others provide support across multiple risk areas. Support may range from simply sharing information and resources to going physically onsite to implement technical solutions and other mitigations.

Finally, organizations should try to determine whether the program will have any public-facing roles or services. Public engagements that raise awareness of existing election security measures may help instill greater public confidence in election operations. Public events could also be an

---

[1] PART 213 CYBER NAVIGATOR PROGRAM: Sections Listing. (n.d.). https://www.ilga.gov/commission/jcar/admincode/026/02600213sections.html

[2] While Minnesota did not require legislation to create their Navigator Program, the state did require legislative approval to spend HAVA funds on the program. For more information, see: Office of the State Of Minnesota Secretary of State. (March 6, 2019). https://www.sos.state.mn.us/about-the-office/

opportunity to solicit feedback on evolving concerns or opportunities for further engagement or product/service development for election officials.

Identify Funding

Funding is a key consideration for implementing a sustainable navigator program. While some states may be able to direct or re-direct existing funds to launch a navigator program, others may need to seek new funds or authorization from the state legislature or other relevant state and local governance authorities. Identifying funds may also be complicated by budgeting and funding cycles that may not align with election cycles. Where available funds are limited, some states first launched a navigator pilot program, to get the program off the ground quickly and demonstrate its value proposition for future budget or program authorization requests.

Federal grants may provide an additional funding source for navigator programs. Help America Vote Act (HAVA) funds, distributed by the U.S. Election Assistance Commission to state election offices, have been used by states to implement navigator programs and other election security initiatives. Department of Homeland Security (DHS) grants, including the Homeland Security Grant Program (HSGP), administered by the Federal Emergency Management Agency (FEMA), and the State and Local Cybersecurity Grant Program (SLCGP), administered by CISA and FEMA, may also be used to advance election security efforts. DHS designated election security as a National Priority Area for the latest round of HSGP funding and included navigator programs as an example in the notice of funding opportunity.[3]

Help America Vote Act (HAVA)	Homeland Security Grant Program (HSGP)	State and Local Cybersecurity Grant Program (SLCGP)
• Provides funding to states and U.S. territories to improve the administration of elections for federal office, including enhancing technology and making certain security improvements • HAVA offers formula grants, discretionary grants, and election security grants. In particular, **discretionary grants** may be a useful source of initial funding to stand up or expand a navigator program	• Provides funding to support the development and continuity of the **National Preparedness Goal** of a secure and resilient nation • The FY 2023 HSGP identified **elections as national priority area** and required recipients to allocate 3% of the award towards election security.	• Provides grants to address cybersecurity risks and threats to information systems used or owned by (or on behalf of) state, local, and territorial governments • The purpose is to assist state, local, and territorial governments with **managing and reducing systemic cyber risk**

Figure 1: Federal Grant Opportunities

Funding opportunities can come from a range of federal, state, and even private sources, depending on availability, need, and state law. Be sure to research all potential options to see what best fits specific navigator program needs.

[3] The Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2023 Homeland Security Grant Program. (n.d.). FEMA.gov. https://www.fema.gov/grants/preparedness/homeland-security/fy-23-nofo

Choosing a Navigator

Like election officials themselves, successful navigators will need a variety of technical, interpersonal, and organizational skills to accomplish the program's objectives. Navigators must also be able to establish trust within their community and initiate new partnerships or collaborations as appropriate for the program.

Key Factors

When choosing an Election Security Navigator, consider these key factors:

- ☐ What are your program's primary objectives and priorities?
- ☐ What are your jurisdictions' main risk factors? Is there a specific area of expertise that would be best for addressing them?
- ☐ What skill sets are most important to accomplish your program's objectives?
- ☐ Are there any individuals with existing relationships or familiarity with your election systems that could easily step into this role?

As the risk landscape shifts, finding a navigator who can understand and effectively support a dynamic election security portfolio is critical. Navigators can always be trained to possess a sufficient level of technical competence across risk domains; however, certain "soft skills," such as effective communication, problem-solving, and adaptability, are also important. States may seek to recruit former election officials or election infrastructure partners as navigators, to take advantage of their institutional knowledge, relationships, and experience. While individuals without prior election experience can still be effective navigators, they may require a greater initial investment of training on working in the election infrastructure sector. These individuals may bring other desired skill sets to the program in specific technical areas that help best accomplish program objectives.

Measuring Performance and Effectiveness

Finally, each state should determine measures of effectiveness to assess the program and identify areas for improvement. When working with a new program, early evaluations can come from anecdotal reporting and counting program statistics (e.g., the number of cases or incidents handled, the number of trainings provided on each relevant topic, how many election workers received those trainings, etc.). **Over time, as the program matures, localities can start to set increasingly ambitious targets for the program and its participants, focusing not just on program outputs, but also on outcomes.** This can also be an effective way to identify what components of the program are most impactful or most in demand. For example, if a particular training or resource proves to be particularly effective, it can be expanded and scaled up for future program needs. Ideally, jurisdictions can rely on these evaluations to help identify areas for improvement and direct incremental changes.

SHARING NAVIGATOR PROGRAM BEST PRACTICES

Information sharing is one of the most important elements of a navigator program. New programs can benefit from identifying core competencies for navigators and existing best practices or resources used in other states and jurisdictions. Local elections officials will likely request assistance on a wide variety of challenges and **all navigators can benefit from sharing information with fellow**

navigators and election officials across states. The power and value of sharing information and best practices is why CISA put this guide together—to increase awareness and understanding of navigator programs nationwide. As navigators look to leverage state and local resources available, they should also remember that Federal partners including FBI, CISA, and EI-ISAC, can also help facilitate connections and share information at a national level.

CONSIDERATIONS FOR IMPLEMENTING DIFFERENT NAVIGATOR PROGRAM MODELS

While all navigator programs differ depending on needs and resourcing, existing programs can be grouped into two general models.

Program Models

Purpose-Built Program Model: some states have created navigator programs from the ground up, addressing election security needs or gaps that were previously unmet. Compared to modified programs (explained below), purpose-built programs may have more flexibility and autonomy to determine navigator role(s) and responsibilities, but may also require more initial funding.

- **Heavy Resourcing**: two or more dedicated navigators
- **Light Resourcing**: one dedicated navigator
- **Volunteer or Intern Resourcing**: programs relying on volunteer or intern support, typically in partnership with one or more universities

Modified Program Model: some states have redirected resources from other existing areas to create navigator programs. These states may already have one or more individuals serving in a navigator-like capacity. Compared to purpose-built programs, modified programs may be easier to launch initially, but may also require the navigators to "dual-hat" with their other roles.

- **Partner Intensive**: programs that rely primarily on partnerships with other entities to provide navigators
- **Shift In Focus**: shifting one or more existing roles within the organization to include navigator activities

Program Considerations

- **Program Scope & Activities**
  - **Scope**: the risk domains that the program may support, including cybersecurity, physical security, operational, and/or disinformation risk domains
  - **Service Area**: based on model and scope, the program will be able to provide services to either some or all election officials within the state
  - **Local Participation**: election officials may engage with the program on a required or voluntary basis
  - **Service Activities**: potential activities that a navigator program may undertake
- **Program Creation & Governance**
  - **Program Creation Authority:** some purpose-built programs may require regulatory approval to be established, while modified programs may be established by organizational leadership directly
  - **Funding Options**: potential avenues for financing navigator programs (non-exhaustive)

  - **Governance**: most navigator programs align to the state's chief election official
  - **Governance Partners**: potential partners for program governance
- **Program Staff & Partners**
  - **Staffing Pipeline**: candidates for navigator programs might be sourced from existing IT professionals; volunteers, students, or interns with IT and/or cybersecurity experience; or existing election security liaisons or coordinators within the state
  - **Primary Staffing Reliance/Scale**: the anticipated number of staff, volunteers, interns, or partners needed to implement the program
  - **Staffing Focus**: candidates for navigator programs may focus on technical expertise, prior elections experience, or professional networks, or a combination of these
  - **Service Provider Partners**: potential partners for program implementation

Table 1: Types of Navigator Programs

Program Details	Purpose Built Programs New programs created for the specific purpose of addressing election security gaps			Modified Programs Existing programs redirect resources to address election security gaps	
	Heavy Resourcing (2+ staff)	**Light Resourcing** (1 staff)	**Volunteer or Intern Resourcing**	**Partner Intensive**	**Shift In Focus**
Program Scope	Basic to intensive support across multiple risk domains	Basic support across limited number of risk domains	Intensive support for a single risk domain (cyber)	Intermediate support across multiple domains	Basic support across multiple domains
Service Area	All Local Election Officials	All Local Election Officials	Some Local Election Officials	All Local Election Officials	All Local Election Officials
Local Participation	Statutory or Voluntary, but driven by grant funding	Voluntary	Required security standards with voluntary support	Voluntary	Voluntary
Service Activities	Information sharing Connecting with service providers Collaborations Needs assessments Trainings and exercises Responding to questions Risk analysis and prioritization Grant support Mitigation guidance Technical implementation Incident response planning COOP Stakeholder engagement Template development	Information sharing Connecting with service providers Collaborations Needs assessments Trainings and exercises Responding to questions Mitigation guidance Incident response planning COOP Template development	Information sharing Connecting with service providers Collaborations Needs assessments Responding to questions Mitigation guidance Template development	Information sharing Connecting with service providers Collaborations Training and exercises Responding to questions Mitigation guidance	Information sharing Connecting with service providers Collaborations Training and exercises Responding to questions Mitigation guidance
Program Creation Authority	Statutory / Regulatory	Regulatory / Management	Management	Management	Management
Financing Options	HAVA Boost / Operating Budget	HAVA Boost / Operating Budget	Operating Budget / Grant Funding	Operating Budget	Operating Budget
Governance	State Chief Election Official	State Chief Election Official	State Chief Election Official	State Chief Election Official	State Chief Election Official
Governance Partners	State IT Information Security Officer (ISO)	State IT ISO	University Program Lead	State IT ISO	State IT ISO

Program Details	Purpose Built Programs New programs created for the specific purpose of addressing election security gaps			Modified Programs Existing programs redirect resources to address election security gaps	
	Heavy Resourcing (2+ staff)	**Light Resourcing** (1 staff)	**Volunteer or Intern Resourcing**	**Partner Intensive**	**Shift In Focus**
Staffing Pipeline	IT Professionals	IT Professionals	Volunteers Interns / Students	Existing Liaisons w/ IT support	Existing Liaisons
Primary Staffing Reliance / Scale	Multiple Staff	Single Individual	Voluntary	Partners	Multiple Staff
Staffing Focus	Technical Expertise / Professional Network	Technical Expertise / Professional Network	Technical Expertise	Elections Experience / Professional Network	Elections Experience / Professional Network
Service Provider Partners	State IT Federal Gov. (CISA) National Guard Private Sector	State IT Federal Gov. (CISA) National Guard Private Sector	Universities State IT Federal Gov. (CISA) National Guard Private Sector	State IT Federal Gov. (CISA) National Guard Private Sector	State IT Federal Gov. (CISA) National Guard Private Sector

CONCLUSION

Now more than ever, states need to draw on every tool in their security toolkit to ensure the resiliency of the Nation's election infrastructure. Navigator programs can serve as a powerful force multiplier to enhance election security at the local level. Many states have seen success implementing navigator programs that are tailored to their election security needs and the nuances of their election administration practices. CISA's Election Security & Resilience team is available to support states interested in establishing or expanding their navigator program and facilitate sharing of best practices across the country.

For more information about navigator programs or other CISA election security resources, please contact ElectionSecurity@cisa.dhs.gov.