THE ELECTIONS GROUP

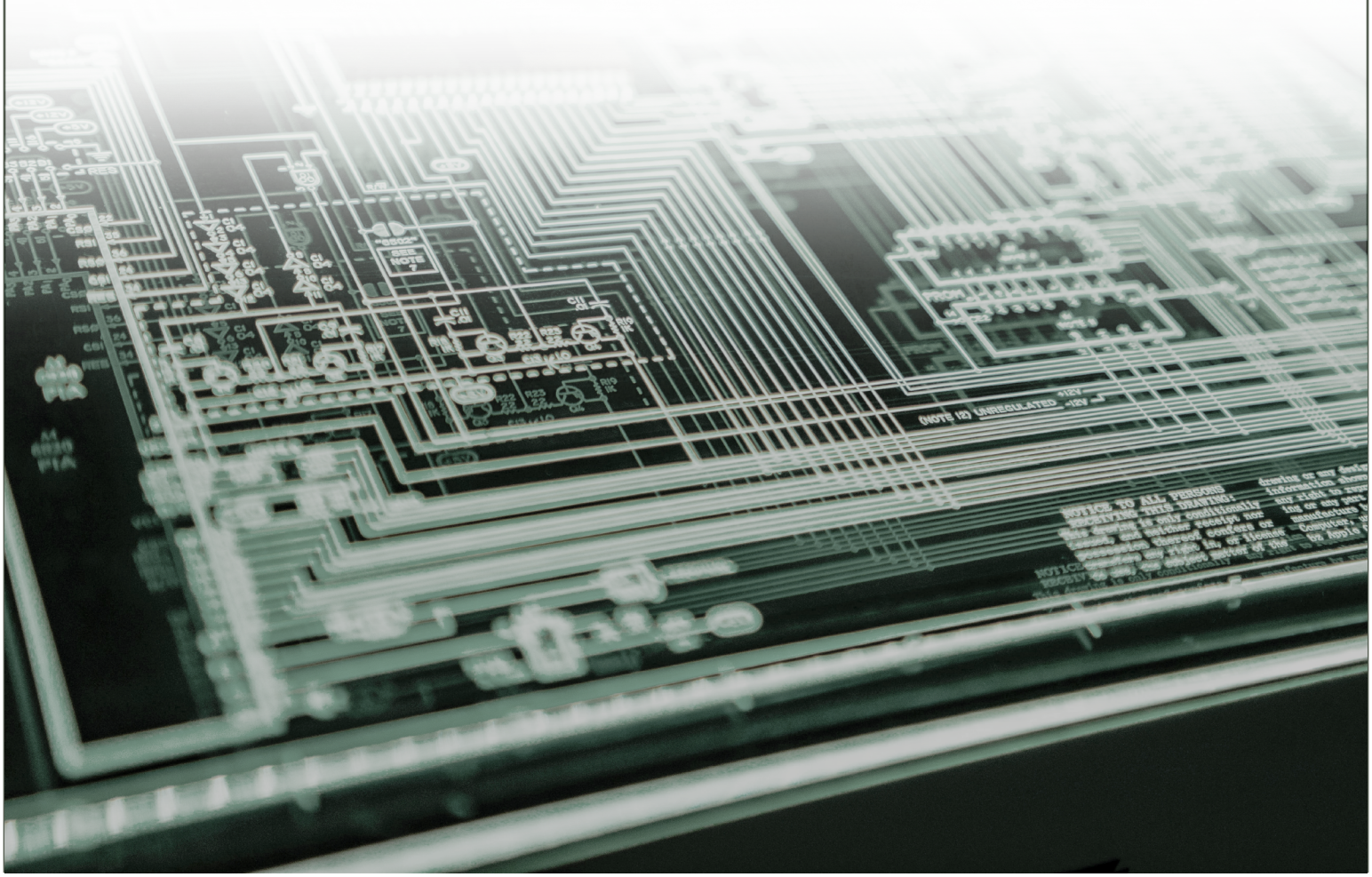
Accelerating Excellence

"3, 2, 1..."

Countdown to a State-Led **Security Navigator Program** to Help Local Election Offices

A Program Implementation Workbook and Reference Guide

Published March 2023



Election security has never been more important. Expanded use of technology has increased vulnerability to cyber attacks. Foreign and domestic threats mean basic levels of physical security for facilities and polling places may be insufficient. Even the sense of personal safety that election officials and workers historically enjoyed has eroded. And, the whirlwind of election information voters receive comes from many sources, some misinformed and some simply working in bad faith. Jurisdictions large and small find themselves overwhelmed.

State officials are positioned to take the lead by developing programs to help local election offices manage these risks. This guide is inspired by the state officials who have already taken the lead in securing elections **by providing advice, support and even direct services to help local election offices (EOs) navigate the unfamiliar waters of election security.**

Whether you envision a quick sprint for existing staff or an ambitious program built from scratch, **this guide can help you achieve results quickly.**

Can State Officials Improve Election Security at the Local Level?

Yes. Several states have already built successful programs. Case studies linked here offer good examples. Each state's plan was different so we've mapped options on a matrix of characteristics to help you develop a plan that can work for your office. (See p. 2 of this guide and compare it to the matrix in each case study.)

How to Use the "3 - 2 - 1... Countdown" Guide

This guide leads you step by step through the stages of building a Security Navigator program.

3

The Planning Phase consists of three steps:

- Defining Key Security Goals and Strategies.
- Structuring Your Program.
- Assembling Partnerships, Resources and Funding.

2

When you are ready to Launch, we guide you through two steps of implementation:

- Writing the Work Plan.
- Onboarding Staff, Partner Organizations and Local Election Offices.

1

And we help you achieve Escape Velocity - Maintaining progress by:

- Reinforcing Success: Setting reachable benchmarks, rewarding achievement, communicating about successes, and then setting more ambitious goals.

Project Scope and Ambition

Breadth and Depth

As you work through this guide, you will complete exercises associated with each line of the chart below. They will help you define the project scope (breadth) and ambition (depth) and choose among options for each project feature – a seemingly overwhelming task in a series of simple steps.

Breadth of Support Offered

	Cyber	Physical	Personal	Operations	Information
Basic					
Intermediate					
Intensive					

Depth of Support

Project Features and Characteristics

Service Strategies	Assessments	Trainings/Exercises	Grant Funds	
	Collaborations	Information Sharing	Hands-On Support	
Program Creation Authority	Statutory	Regulatory / Rule-Making Authority	Discretionary Authority	
Local Participation	Statutory Mandate	Voluntary but Funding-Driven	Entirely Voluntary	
Financing	Federal Funds	State Funds	Other Funds	Mixed Financing
Staffing / Scale	Single Individual	Multiple Staff	Partnerships	Voluntary Providers
Staffing Focus	Security Subject Matter Expertise	Relationship Builders	Elections Expertise	
Partners	Federal Agencies	Other State Agencies	NGOs	
Collaboration Approach	Top - Down	Collaborative: Advisory Board; Roundtables; Working Groups		
Assessment Tools	NIST	Cybersecurity Framework	CIS Controls	Other

3, 2, 1

Planning Your Security Navigator Program

*To plan your security program, **the countdown to launch includes these steps:***

Define Key Security Goals and Strategies

Structure Your Program

- Determine the Authority to Create the Program
- Identify Local Participation Requirements
- Develop a Plan for Staffing and Service Providers

Assemble Partnerships, Resources and Funding

As you proceed through the exercises below, **think broadly about the risk environment**.

- Your vulnerabilities,
- The likelihood of an incident,
- The severity of the consequences.

Then zoom in on the concerns that are most pressing and least likely to be addressed by EOs or other agencies.

We reviewed a number of state programs for our case study series. No state tried to address all security domains. Inevitably, **you will narrow your focus based on your capacity**.

Planning vs. Implementation

"I have always found that plans are useless, but planning is indispensable."
- President Dwight Eisenhower

The exercises in this guide can help by making you aware of choices and priorities, preparing you to adapt as circumstances change.

Defining Key Security Goals and Strategies

Your program should address the most critical risks where you can offer support to local election offices (EOs). We offer a series of exercises starting at a high level, zooming in to consider what is most pressing and practical, then zooming back out to ensure you're addressing your high-level priorities.

- **Exercise A** - Assessing High-Level Risk Across Different Domains of Security
- **Exercise B** - Identifying Specific Vulnerabilities
- **Exercise C** - Analyzing Risk - Vulnerabilities Ranked by Likelihood and Impact
- **Exercise D** - Brainstorming Strategies to Address Specific Concerns
- **Exercise E** - Aligning Strategies with Risks

Exercise A

Assessing High-Level Risk Across Different Domains of Security

A first pass at risk assessment is to assess the general readiness of your jurisdictions by considering risk across five distinct security domains.

Cybersecurity – Are computer systems, hardware, software and data storage adequately secure against penetration, information harvesting, and tampering?

Physical Security – Are offices, operation facilities and voting sites secured against disorderly protest and/or attempts to enter unlawfully? Are voting systems, ballots and other materials protected from unauthorized access?

Personal Safety – Do election officials, staff and poll workers feel safe from harassment and threats of violence? Do they feel secure in the office, at home and en route?

Election Operations – Are standard operating procedures in place to ensure uniformity and limit mistakes? Are two-person or bipartisan custody requirements used to deter insider threats? Are chain of custody standards sufficient to document security?

Election Information – Is there capacity to inform the voting public, both proactively and in response to mis- & disinformation campaigns?

Gut Check vs. Analysis

This first pass is a high-level gut check - what do you think are the biggest security domains?

Later in the guide, we offer tools for deeper analysis of risk. Comparing that analysis to your gut check will ensure the details do not distract you from larger purposes.

Risk Assessment Across Different Domains of Security

In each column, make an X in the row reflecting the risk in that security domain.

Level of Risk	Cyber	Physical	Personal	Operations	Information
Manageable					
Moderate					
Significant					

Exercise B

Identifying Specific Vulnerabilities in Election Offices

In this chart, **circle five to eight issues** that represent the most pressing risks your jurisdictions face. (Add other issues at the bottom as needed.)

Identifying Specific Vulnerabilities in Election Offices

Cybersecurity	Physical	Personal	Operations	Information
Insecure systems, hardware and data	Office space not designed for security	Fear among staff, poll workers	Poor/inconsistent ballot accounting or chain of custody practices	Inability/uncertainty responding to mis/disinformation
Unsafe internet and computer use/practices	Limited resources	No reporting system for threats, security incidents	Insider threats	Deifficulty grabbing attention from media/wider media market
No cybersecurity standards	No risk assessment capability	No protective services plan with law enforcement	No crisis planning or insufficient planning	Lack of communications staffing and resources
Backup systems missing or insufficient	Law enforcement partnerships undeveloped	No resources (security cameras, alternate housing for employees during incidents)	Staff turnover	Inconsistent policies (e.g., chain of custody) hinder communications about transparency, integrity

Exercise C

Analyzing Risk - Vulnerabilities Ranked by Likelihood and Impact

Create a risk analysis by taking the issues you identified in the previous chart and ranking them according to their likelihood and potential impact.
(Include the Security Domain that each falls under – Cyber, Physical, etc.)

	Security Domain	Specific Risk
e.g.	Information	Lack of communications staffing & resources
1.		
2.		
3.		
4.		
5.		
6.		
7.		

Colorado leaders initially planned for a Navigator Program focused on cybersecurity issues that emerged in 2016. Risk analysis led them to recognize that disinformation efforts were growing beyond the capacity of local or state officials to respond. "We didn't have enough horses," said Judd Choate, the Director of Elections for the Secretary of State.

By ranking the specific risks previously identified, you've identified **critical risks** for election offices in your state. Depending on resources, you might decide to draw a line and address only the most critical issues, ranked higher in your list.

Exercise D

Brainstorming Strategies to Address Critical Risks

For each problem identified, consider what programs and services are most likely to improve the security posture of EOs.

To facilitate brainstorming, consider this spectrum of service strategies from basic to intensive.

Service Strategies

Assessments	Info-Sharing	Trainings & Exercises	Grant Funding	Collaborations	Assessments

With that range of service strategies in mind, **list the Critical Risks from Exercise C in the table below**, and then fill in service strategies your state program is considering to address them.

In Illinois, Navigator Program Manager Amy Kelly encourages interested jurisdictions not to get overwhelmed with the scope of their efforts. "My number one piece of advice would be to remember that even small changes have a huge impact."

Brainstorming Strategies to Address Critical Risks

Specific Risk	Strategy 1	Strategy 2	Strategy 3
Example - Office space not designed for security	State-run security assessment working with State Police	State-led working group sets physical security standards	Matching grant funding for improvements

Exercise E

Aligning Strategies with Risks

In Chart C, you prioritized risk in one or more Security Domains, and in Exercise D, you brainstormed strategies to address them. Now complete the Program Emphasis chart below, **marking an X in each column** to reflect how many strategies address risks in each Security Domain.

For instance, if you listed three cyber issues and a mis-/disinformation strategy, you might mark Cyber as Intensive and Information as Intermediate or Basic, leaving the other columns blank.

Program Emphasis for Each Security Domain

	Cyber	Physical	Personal	Operations	Information
Basic					
Intermediate					
Intensive					

Adjusting Goals and Strategies to Fine Tune Your Plan

Notice how the Strength of Focus chart is similar to the Risk chart from Exercise A. Do your priorities still line up with your original assessment of needs?

For instance, if Cybersecurity and Personal Safety are the most critical risk domains, then you should have developed a strong set of strategies to address them.

If your Strength of Focus (Chart E) does not align with your Risks (Chart A), your program emphasis may not meet your strategic goals.

Comparing Risk (Chart A) with Focus (Chart E)

Risk Assessment

	Cyber	Physical	Personal	Operations	Information
Basic		X		X	
Intermediate					X
Intensive	X		X		

Strength of Focus

	Cyber	Physical	Personal	Operations	Information
Basic					
Intermediate					
Intensive	X		X		

If your assessment of risk has evolved, adjust the Risks (Chart A) to reflect your new assessment.

If you still agree with your initial risk assessment, consider whether there are issues you did not list in Exercise B, or additional strategies you might add to Exercise D, to align program goals and strategies with your high-level risk analysis.

Structuring Your Program

With goals and strategies established, you need to plan for governance and oversight, then write a charter for the program. Key aspects will be to:

Determine the Authority to Create the Program

- Establish the legal basis under which it will operate

Identify Local Participation Requirements

- Approach collaboration productively
- Define the state/local relationship
- Identify ideal attributes of a program manager

Develop a Plan for Staffing/Service Providers

- Envision your program manager and staff

Compile Key Components into a Draft Charter

Determine the Authority to Create the Program

Before moving forward, it is important to define the legal basis for your program, and possibly pursue legislation to establish one.

Program Creation Authority

Statutory	Regulatory / Rule-Making Authority	Discretionary Authority

Differences in state authority to create a program could impact not only whether you can launch a program, but also budgetary issues and the degree of compliance by EOs.

Some state officials have the independence, budgetary flexibility and rule-making authority to move forward with a strong Security Navigator program.

Others, with more limited jurisdiction over EOs, might **pursue statutory authorization** or a collaborative effort that may rely on a committee structure rather than hiring additional staff.

Colorado
Legal Authority

- The Secretary of State has broad rule-making authority over election administration.
- No additional legal basis was necessary.

Exercise F

Establish a Legal Basis for the Program

Describe the legal foundation for your program. If legislation may be required, list requirements to be incorporated. Give particular thought to the Strategies chart (Step One, Exercise D). Do these strategies require statutory changes?

Illinois

New Legal Authority Sought

- The Illinois State Board of Elections (SBE) had limited rule-making authority,
- Without a new statutory requirement, the state would not have created a Navigator program.

North Carolina

Discretionary

- Counties were receptive to the largely collaborative "HUBS" program ("Helping Us Be Successful")
- The North Carolina SBE felt that no new enabling legislation was required.

Illinois: Supporters Pass Statute Mandating Navigator Program; Making Grants Contingent on Participation

The Board shall adopt rules, after at least 2 public hearings of the Board and in consultation with election authorities, establishing a cyber navigator program to support election authorities' efforts to defend against cyber breaches and detect and recover from cyber attacks.

The rules shall include the Board's plan to allocate any resources received in accordance with the federal Help America Vote Act and provide that no less than half of any funds received under the federal Help America Vote Act shall be allocated to the cyber navigator program.

The cyber navigator program shall be designed to provide equal support to all elections authorities with some modifications allowable based on need.

The remaining half of the federal Help America Vote Act funds shall be distributed as the Board sees fit, but no grants may be made to election authorities that do not participate in the cyber navigator program managed by the Board.

From the Illinois Election Code, 10 ILCS 5/1A-55

Identify Local Participation Requirements

Closely related to the legal basis for creating a program is the degree to which compliance by EOs can be compelled or encouraged. Some different approaches are listed below.

Local Participation Requirements

Statutory Mandate	Voluntary and Funding-Driven	Entirely Voluntary

Participation can be

- **Mandated** by the state, by legislation or by rule-making authority
- **Incentivized**, using grant funding or other benefits to encourage participation
- **Entirely voluntary**, particularly if a collaborative approach encourages mutual respect and a shared approach to problem-solving
- **A combination** of any of the above

Collaboration is helpful no matter which legal model is followed.

Participation and adoption of practices and products can be voluntary.

A state mandate can provide a powerful incentive for constructive collaboration, whether specific outcomes are written into law, granted through rule-making authority or vested in working groups.

Illinois
Voluntary & Funding-Driven

- Participation is incentivized through grant funds tied to legislative requirements.
- A 2016 security breach made participation urgent.

North Carolina
Entirely Voluntary

- Participation in HUBS working groups
- Adoption of HUBS products and compliance with HUBS standards
- Relatively unobtrusive guidelines encourage commitment from locals.

Virginia
Standards-Driven

- A 2019 legislative mandate that EOs meet minimum cybersecurity standards incentivized participation.
- Navigators, who are IT students trained in assessing systems and implementing best practices, offer EOs a cost-effective way to meet those standards.
- Smaller jurisdictions with limited IT resources had the strongest incentive.

Approach Collaboration Productively

Whether or not participation is required, a collaborative approach will improve content and encourage adoption. EO input can help prevent the program from moving in directions that are impractical or impossible to implement. Collaboration can drive the program in new directions as EOs recognize the efficiency of drawing on both pooled and state resources.

Collaboration Approach

Collaboration can move forward in a variety of ways.

- **Advisory Boards**, reflecting the diversity of EOs large and small, rural and urban, can guide a staff-driven program and prevent potential missteps.
- **Participatory working groups** can give EOs both practical and decision-making authority.
- **A roundtable** that engages every EO can set security standards by consensus. The give and take of meetings provides EOs with a sophisticated understanding from which to pursue independent solutions.
    - This is more practical in states with fewer EOs.

"First Contact"

Military planners remind themselves that "No plan survives first contact with the enemy." EOs aren't enemies. But your plan will be transformed when EOs make contact with it. Be flexible enough to accept their constructive ideas and they will strengthen your program.

Virginia
Advisory Board

- The SBE was given a mandate to create a Voter Registration System Security Advisory Group consisting of state and local election officials and local IT staff.
- Cybersecurity standards that EOs are required to meet emerge from this collaborative group.

North Carolina
Working Groups

- At the heart of the HUBS program are individual "HUBS" – working groups of volunteers from EOs.
- Large and small jurisdictions, and both experienced employees and newer staff with fresh eyes, sit on each HUBS team.
- With different HUBS addressing a range of issues (election security, and many operational topics as well), all 100 counties find a place.
- A steering committee consisting entirely of SBE staff, including the director and deputy director, oversees the HUBS program.

Early Collaboration tips:

- **Enlist "anchor tenants,"** popular, influential officials who see the benefits of a consistent statewide approach.
- **Recruit leaders** from your state association of election officials.
- **Share ideas and details with allies** to get feedback and improve the plan before any wider launch. Such allies may even support a push for legislation or rule-making authority.

Defining and Refining Goals

Exercises in Phase I helped identify your goals. Consider working through those same exercises again with an influential local election official you trust or a small group to help align your goals and theirs.

Arizona
Standards-Driven

- Led by a staffer of the Secretary of State, a roundtable of election and IT staff from each of the state's EOs meets regularly to discuss cyber- and related security issues.
- Conducts table-top exercises (role-playing wargames common in the security field).
- Policies are developed by the group and implemented locally.
- Although the state program has little statutory authority, strong state leadership has been influential in guiding the program towards meaningful solutions.

Top-down mandates like Virginia's may be necessary to ensure all EOs adhere to minimum standards. Though existing rule-making authority may allow enforcement of standards, it still may be useful to advance legislation specifically authorizing the state election office to create new security policies.

Whatever type of collaborative relationship is envisioned, the kickoff meeting with EOs will be critical in determining the attitude EOs adopt towards the program. Giving them a sense of how they can participate will allay their concerns and encourage a constructive cycle of feedback.

Exercise G

Defining the State / Local Relationship

1. Describe the relationship between the program and EOs, including how they will be encouraged, or required, to participate, and the type of committee or workgroup(s) in which they will collaborate or offer feedback.

2. Is this consistent with the current relationship, or does it reflect a change? How will you incentivize and manage that change? Do some of the strategies you outlined in the Phase I Strategies chart (Exercise D) fit better than others within the existing relationship?

3. Describe how program leaders and staff will interact with EOs to develop standards and procedures. Where will decision-making authority rest? Will standards be mandated, voluntary or encouraged by offering benefits for EOs that comply? Is new legislation or rule-making authority necessary to ensure compliance?

Identify Ideal Attributes of a Program Manager

The qualities necessary to lead the project are linked to the goals, the number of staff and their relationship to EOs and other partners.

Your program might require a candidate with strengths in one of these areas:

- An extensive security background
- Existing relationships with election officials
- People skills and experience with oversight and motivation
- Managing relationships with a variety of EOs, staff, partner organizations and political constituencies

Illinois
An Election Professional

- The SBE emphasized motivating compliance from 108 offices, mostly run by elected officials with a history of independence from the state.
- They promoted a program manager with extensive SBE experience working with EOs around the state.

Virginia
A Project Planner

- For a program relying on academic partners, grants from the National Security Agency and placement of interns across a dozen counties, the SBE promoted an in-house manager whose pre-SBE experience was in private-sector project planning and human resources.

Colorado
A Security Professional

- Colorado hired an analyst from a federal security agency to direct a program prioritizing disinformation.
- That director in turn hired a small number of staff experienced in physical and cybersecurity.

New Jersey
A State Security Official

- New Jersey's program expanded on an existing cybersecurity initiative in the New Jersey Office of Homeland Security and Preparedness (HSP).
- New Jersey employs a single dedicated Election Cybersecurity Coordinator in a navigator role.
- The coordinator is supervised by a cybersecurity expert in HSP with a strong relationship with the Secretary of State's Election Division.

Develop a Plan for Staffing / Service Providers

There are a variety of different **staffing strategies, ranging from dedicated IT professionals or college tech majors to election staff with relationships.**

Staffing Focus

Security Subject Matter Expertise	Relationship Builders	Elections Expertise

Staffing and Provider Plan

Single Individual	Multiple Staff	Partnerships	Voluntary Providers

Staffing your program is linked to how it has been defined thus far:

- How **ambitious** are its **goals**?
- Are you **harvesting low-hanging fruit**, a set of simple improvements that EOs have not dealt with?
- Do you need in-depth **technical understanding**?
- Will staff need to **manage relationships** carefully to motivate EOs, or is there a statutory backstop encouraging cooperation?
- Available funding.

Your answers will dictate the type of staff needed, recruiting strategies and the nature and depth of staff training.

Many programs prioritize existing relationships with elections officials or strong relationship-building skills because much of security work is about bringing everyone above the groundwater line by implementing basic safeguards. **Mutual trust and recognition can help program staff fit security work into the value structure and workload of local EOs**. Existing state election staff may have the skills and relationships necessary.

Colorado
Security Expertise

- Colorado's three-staff unit included a director from the national security arena and two specialists in cybersecurity and combating disinformation.
- The former director recommends recruiting ex-military or law enforcement who will approach the job with a ready understanding of the types of penetration attempts and threats they are defending against.

Virginia
Building Election Knowledge into an IT Curriculum

- College students with IT-related majors take a boot camp to learn about election administration and the key election cybersecurity issues.
- After boot camp, each student is assigned to support an EO.

The simplest path to launch could be expanding an existing liaison or compliance program by adding a security focus. Or, by recruiting staff from EOs, you may find candidates with both elections and IT experience (taking care not to undercut valued local partners).

> If you focus on technical skills, as many programs have, **an elections "boot camp" may be helpful in orienting IT staff to the work.**

Some states take a regional (Illinois) or even local (Virginia) approach to service provision, assigning personnel to given counties or parts of the state, though recruiting and assigning cybersecurity experts by region can be difficult.

By recruiting staff from EOs, you may find candidates with both elections and IT experience (obviously taking care not to offend your EO partners in the process). But most **experienced election staff are likely to need an immersive experience in security techniques** in order to understand the measures they teach EOs to implement.

To build a team with the right mix of skills and knowledge, you will need to plan training carefully to assemble the mix of specialties required.

A number of **states have turned to a college or university to build their training program**. Other states enter agreements with private, non-profit or academic providers for a range of specific services, a topic we touch on in the next section "Resources, Partnerships and Funding."

Exercise H

Envisioning Your Program Manager and Staff

1. List attributes and skills your program manager will need to succeed. In particular, consider the mix of security expertise, elections experience, relationship-building and personnel management in an ideal manager.

2. Looking back at the goals and service approaches from Step One, consider the number and type of staff that may be necessary to achieve program goals.

3. Take time to consider how the skills and expertise of staff may need to complement those of the program manager. A candidate who already has relationships with EOs may smooth the path for security-oriented staff, while a subject matter expert as manager may need liaisons to EOs.

4. List key aspects of the training and orientation that will give staff the knowledge to build constructive relationships with the EOs.

5. Consider whether existing programs and/or staff duties within the office can be modified to offer some basic levels of support. For example, a liaison program currently verifying compliance with statutory filing requirements, or testing election night reporting files, could be modified to share security information or help EOs request free services from other providers.

Exercise I

Compile Key Components into a Draft Charter

Reflecting on what you've written in the previous Structuring Your Program exercises, compile key components into a draft charter for your program

Draft Charter for the Navigator Program

- Legal Foundation
- Relations between the State and Local EOs
- Key Characteristics of Program Manager and Staff

Your Draft Charter

Assembling Partnerships, Resources, and Funding

Some partnerships can be foundational. A state office of emergency management could play a key role in your program, or you could encourage EOs to look to their own emergency management offices for support.

Other partnerships play a more supplemental role, providing a few key skills and services at low (or no) cost:

- Many states rely on the U.S. Cybersecurity and Infrastructure Security Agency (CISA), or the National Guard for risk assessments.
- Other states partner with local or state law enforcement or EMS agencies for physical security walk-throughs and other services.
- In some cases, NGOs may also provide narrowly-tailored support.

Think through what other agencies and organizations may help fill gaps in your own agency's capabilities and provide economical alternatives to developing a skill set in-house.

Virginia
A Broad Academic Partnership

- Partnership with universities is central to Virginia's Navigator program.
- They provide instructional support as well as a pipeline of IT-focused interns.

New Jersey
A State Security Agency Partner

- The state Division of Elections looked to the New Jersey Office of Homeland Security and Preparedness to house and oversee the election security program.

Iowa
A Narrow Role for the National Guard

- The Iowa Guard's Joint Task Force Cyber was tasked with cyber threat monitoring for elections, working alongside the state Department of Management.

Indiana
A Tightly Focused Academic Partnership

- The Voting System Technical Oversight Project (VSTOP) is Indiana's tightly focused partnership with Ball State University.
- Two professors from the Computer Science and Political Science Departments provide technical expertise for voting system certification.

Partners

Federal Agencies	Other State Agencies	Non-Governmental Organizations

Resources

A successful program will need many resources. Some tools you may need to find, borrow or develop include:

- A staff orientation manual and/or training aids
- Risk assessment tools
- Security best practice guides and checklists across all domains of security you choose to address – cyber, physical, personal, operations and election information
- Methods of compliance review or post-implementation testing

The states that have already launched Navigator programs will be an excellent source of materials. **Consult the collection of Navigator Case Studies at our website** (https://www.electionsgroup.com/accelerating-excellence) to find states with programs similar to what you envision. Feel free to ask us at the Elections Group for contacts in the states.

Funding

Estimate Costs

You will need to assess the program's structure, staffing and resources, to estimate how much your program will cost.

Identify Potential Sources of Funding

Consider whether funding is available within the agency, or whether you need new authorization from the legislature. Federal and other grant funding has also been used for navigator programs.

Financing

Federal Funds	State Funds	Other Funds	Mixed Financing

Review Your Planning:

1. Does the program as drafted have the capacity to address the security issues you identified?
2. Is it funded, or are there realistic prospects for obtaining funding?

North Carolina
Distributing Costs

- With local EO working groups shouldering much of the workload, SBE costs were limited.

If either answer is no, you may need to zero in on the most glaring risks, limit your program to only one or two of the domains of security, trusting the rest to EOs, or addressing them only with basic information provided at a low cost to your agency, or move to a more collaborative model.

Virginia
Prioritizing Need

- The Virginia Cyber Navigator Program accepted 17 counties in its first year, including some whose vulnerabilities were deemed significant.
- The SBE expects to cycle through all EOs over several years.

Colorado
Prioritizing a Risk Domain

- Colorado focused energy on building a powerful campaign against election disinformation in its early phase.
- The state expects to pursue a stronger emphasis on direct work with EOs in coming years.

Illinois
Grants Fund an Ample Staff

- Illinois used HAVA grants to hire a director and eight staff with security backgrounds.
- The staff work on a regional basis, developing strong relationships with their local EOs and providing direct support and services.

Iowa
Casting a Big Shadow with a Small Program

- Budget considerations led Iowa to hire just one coordinator.
- The coordinator works closely with an IT staffer at the Iowa State Association of Counties to develop cybersecurity educational materials and guidelines, communicate them to EOs and encourage compliance.

Structuring Your Program - Final Thoughts

Your anchor tenants, EOs, program manager and staff will likely alter not only the details of implementation, but the goals and methods. As you move forward, **make a conscious choice to embrace their feedback**. Accepting and incorporating their good ideas will improve your program.

3, 2, 1

Launch: The Program Gets Underway

As the launch approaches, create a project timeline for the first year with key stages:

Writing the Work Plan

- Create a Program Management Timeline.
- Present Work Agendas and Initial Assignments.
- Perform a Risk Assessment.

Onboarding Staff, Partner Organizations and Local Election Offices

- Train Staff and Service Providers.
- Onboard Local Election Offices.

Writing the Work Plan

Create a Program Management Timeline

The timeline for the opening phase should include **all major tasks related to program development**, as well as b**enchmark dates for meeting objectives** like completing risk assessments, developing standards and assessing performance/compliance.

- Hire/assign a program manager.
- Define roles of partnering organizations.
- Finalize staff/intern job descriptions and begin recruiting.
- Hire staff.
- Train staff.
- Onboard election offices.
- Establish risk assessment methodology.
- Begin task group meetings.
- Develop security standards in conjunction with EOs.
- *Hold feedback meetings on efforts to meet standards.
- *Perform a compliance assessment

** We discuss these tasks in the final section "Maintaining Your Success."*

The steps in our timeline at left are suggestions. Adjust them to match the details of your plan and will vary by the nature of your program.

- If your plan is collaborative, like North Carolina HUBS, the step we call Begin Task Group Meetings might indicate the date when each HUBS team first meets.
- In an Illinois-style, staff-led security training and support program, it might indicate the start date for face-to-face meetings with EOs to conduct risk assessment.

Exercise J

Create a Management Timeline

Taking the bullet points above as a starting point, list critical steps for your program and fill in target dates:

	Task	Target Date
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

Present Work Agendas and Initial Assignments

At the introductory meeting, present goals in an inspiring way, explain the expected timeline and solicit cooperation. To take advantage of any excitement, be ready with explicit work assignments and roles.

Sample Agenda

- A staff orientation manual and/or training aids
- Introduce project goals.
- Build consensus around the state's most pressing vulnerabilities.
- Recruit EO volunteers for an oversight committee or work groups focused on specific security topics, as venues where they can provide feedback and shape the program.
- Explain plans for risk assessment, seeking feedback.
    - Schedule site visits.
- Present any tools you plan to use in risk or compliance assessment.
- Schedule a tabletop exercise to reinforce understanding of procedures in the domain(s) of security your plan addresses.
    - Consider whether EOs or staff might help organize and run a tabletop exercise.
- Present communications ideas and elicit EO feedback on themes and issues they want addressed.
    - Credit EOs and the program as successes are achieved.
    - Strengthen public perceptions of the integrity of your state's elections.

> Details may be less important than demonstrating action and forward motion.

Perform a Risk Assessment

Since risk assessment is likely the first significant project you can undertake, adopting a risk assessment tool, by selecting or adapting an existing assessment tool or developing one internally, is an important part of the program rollout.

Risk Assessment Tools in the Cybersecurity Domain

NIST	Cybersecurity Framework	CIS Controls	Other

Excellent cybersecurity assessment tools already exist for you to use or adapt (see our list below). In other security domains, you may need to draft your own checklist, incorporating safeguards and procedures you can find in best practice guides.

Resources in the Five Security Domains

To build a baseline assessment checklist, look over some of the following documents and pull five or ten priority items for your EOs.

> The risk assessment tool helps guide the work of IT contractors who cycle through the office, ensuring that each new contractor is "checking more boxes off the list."

Cybersecurity

- Nationwide Cybersecurity Review - a tool developed by the Multi-State Information Sharing and Review Center (MS-ISAC).
- Cybersecurity Framework Election Security Profile – a "roadmap to prepare for and respond to cyber threats that could affect elections" from the National Institute of Standards and Technology (NIST)
- Cybersecurity Tool to Protect Elections – a "toolkit of free tools to help state and local election officials and vendors enhance cybersecurity" developed by the Cybersecurity and Infrastructure Security Agency (CISA)
- Election Infrastructure Cyber Risk Assessment (CISA)
- Essential Guide to Election Security (CIS)
- The Cyber Security Evaluation Tool (CSET)

Physical Security

- CISA SAFE Fact Sheet - A CISA program sends staff on site visits to evaluate facilities, identifying effective existing practices and areas that can benefit from additional attention.
- Infrastructure Survey Tool - (CISA)

Personal Safety

- Mitigating the Impacts of Doxing - (CISA)
- Running Elections Without Fear - Ensuring Physical Safety for Election Personnel - (The Elections Group)
- Defending Democracy - Protecting Elections Officials from Digital Threats - (The Elections Group and Security Positive)
- 7 Quick Simple Election Safety Tips - (The Elections Group & the Brennan Center for Justice)

Election Operations

- The Elections Group Resource Desk - This library of resources includes a number of guides to specific election processes, with chain of custody forms and guidelines that can help secure election operations.

Election Information

- Developing a Crisis Communications Plan - (Elections Group)
- Election Cyber Incident Communications Guide - (Belfer Center)
- Cyber Incident Detection and Notification Planning Guide - (CISA)

Onboarding Staff, Partner Organizations and Local Election Offices

Train Staff and Service Providers

In Phase III – Planning, we offered some ideas for recruiting staff and seeking assistance from organizations that may be able to provide security services. Here, we give more detail on bringing them in and preparing them for the project through training and orientation.

Staff will likely come from a mix of elections and security or IT backgrounds. Regardless of who you choose, **they will need orientation to the challenge of shepherding EOs who value their independence into complying with standards that are quite technical.**

Training Security-Minded Staff

Orienting security-minded staff to the election environment is a multifaceted challenge. Security staff will know little more about elections than the average citizen and **significant parts of what they think they know about elections may be wrong**.

Training on the election environment should start from a basic level. One way of approaching training which may provide a familiar template is by breaking major election topics down into processes, the systems that support those processes and the existing safeguards and controls. For instance:

General Outline

Training Topic
- [Process]
  - [System / Method]
    - [Safeguards and controls]

Example

Voter Registration and Voter Rolls
- Voter must register
  - Online VR website
    - Internet security controls

For each election system, describe risks and safeguards. **Grounding the discussion in the recent history of election security incidents in your state** and nationally will help them understand the types of threats they should anticipate and prepare for. They will also need to see the contours of risk across jurisdictions large and small, rural and urban. Knowing the structure of election administration in your state – which offices and agencies are responsible for what – is imperative.

You may find it helpful to provide **a glossary of common election terms** and concepts. Whether your state uses polling place or voting site, observer or poll watcher, new security staff should recognize the basic vocabulary that every election staffer and politico knows. We can't list them for you because many terms will be unique to your state or region.

Defining and Refining Goals

In addition to common election terms that security hires may not know, many states have their own jargon. One of our favorites is a forms-and-supplies container known in Pennsylvania as "the shirt box". Imagine the reaction of a security staffer asked how to ensure chain of custody for the shirt box.

Training for Election-Oriented Staff

If you choose to bring on staff with election experience, you will need to train them on a general approach to security and the specific standards, safeguards and controls you intend to establish. The Illinois SBE found it effective to draw parallels between cybersecurity and basic concepts of home security. We recommend drawing topics from and building lessons around the best practice guides in the Risk Assessment section below.

Outside Organizations

If you are working with other service providers, such as outside agencies, universities or private entities, **you need to finalize contracts or prepare memorandums of understanding** outlining the agreement between the two agencies. In other ways, outside agencies may be in a similar position to new employees – they too may need to be oriented to the election environment to dispel misunderstanding and prepare them to work with local EO staff.

> The HUBS program "created a collaborative place with multi-directional energy," North Carolina SBE Director Karen Brinson Bell says.

Onboarding Local Election Offices

Onboarding election offices presents a different challenge. **Some EOs will join a Navigator program enthusiastically.** You may have even brought in some of these as "anchor tenants" or as part of an organizing committee. Other EOs may recognize the need to strengthen their security procedures. But it is likely that a few may approach the program unenthusiastically, or cling to their independence from state leadership. The SBE director in North Carolina believed that collaboration and local ownership helped the program achieve "multi-directional energy" that helps carry along the reluctant.

We recommend approaching onboarding with a sense of the **multiple potential motivations of EOs.** They may be lured by the incentive of grant money, inspired by a vision of excellence, interested in building unity with neighboring EOs, attracted by the possibility of good press or motivated by greater community understanding of election integrity.

You will also need to consider the diversity of your EOs. At the simplest level, this means identifying appropriate contacts. Depending on the nature of your project and the size of the county, **the EO contact might be the officeholder, the appointed election director, an internal IT or Chief Information Security Officer,** county IT staff or CISOs or someone in a county public safety office.

> "We worked our tails off," Illinois Navigator manager Amy Kelly said, of traveling to each county to reassure local leaders the state intended to support their security efforts, not override them.

Your onboarding process for EOs will have to deal with this diversity of organization and motivation. Whether you roll out the program at a state meeting or visit offices individually, consider what impressions, positive or negative, your contacts may bring to the meeting and how to speak to their motivations to build a constructive team.

3, 2, 1

Escape Velocity: Keep the Program Moving Forward

To achieve success, your Navigator project will need to make ongoing progress towards meeting a set of security standards.

Reinforcing Success

- Set Ambitious, Realistic Standards
- Reward achievement
- Communicate about successes
- Set more ambitious goals

Standards are the endpoints that help ensure compliance and create a body of evidence you can point back to. By defining **benchmarks—midpoints on the road to completion**—you can keep the project on track and convince participants their efforts are constructive and not futile.

> Each benchmark met is an opportunity to **reward acheivement, build a narrative of success and reinforce the commitment of all participants to their community of interest** in improving election security.

Set Ambitious, Realistic Standards

The tools listed in Phase II – Launch: The Program Gets Underway can help you define security standards, but you will need to **adapt these model standards to your state's environment.**

Program leadership can write standards or recruit stakeholders to develop them. Cybersecurity in particular may lend itself to a top-down process because of the technical nature of the domain and because **vulnerabilities in a single EO have cascading consequences** across all the jurisdictions in your state.

To date, the strongest single source document that seeks to advance security across all risk domains is the Essential Guide to Election Security (CIS).

We can't begin to list all the standards you may choose to implement. The table below offers examples of the types of standards you might write in each domain, and shows how to set more ambitious targets for EOs at a higher maturity level.

Exercise K

Draft Your Security Standards

	Baseline Standards	Advanced EO Standards
Cyber Security	**Sample:** ☐ Create an inventory of all hardware and software assets ☐ Etc.	**Sample:** ☐ Implement software tools ● to discover devices on your network ● to prevent unwanted software installation
	Add Your List of Cyber Security Standards	
Physical Security	**Sample:** ☐ Create secure space for storage and preparation of tally-related equipment ☐ Log access to secure space with sign-in forms ☐ Require two staff to be present	**Sample:** ☐ Intall camera coverage ☐ Install swipe card access for digitally logging
	Add Your List of Physical Security Standards	
Personal Safety	**Sample:** ☐ Speak to local law enforcement before each election ☐ Set routine security expectations	**Sample:** ☐ Adopt a formal security plan ☐ Practice the plan
	Add Your List of Personal Security Standards	
Operations Security	**Sample:** ☐ Use chain of custody forms when moving any sensitive materials ☐ Adopt two-person or bipartisan standards for sign-off on chain of custody forms	**Sample:** ☐ Continuously monitor your security measures for adherence including reviewing access logs ☐ Routinely audit chain of custody documentation for adherence to policy and accuracy
	Add Your List of Operations Security Standards	
Security Communications	**Sample:** ☐ Prepare a template press release for response to disinformation attempts	**Sample:** ☐ Deploy a rumor control web page
	Add Your List of Cyber Security Standards	

Benchmarks

Benchmarks help participants recognize their own work and the state's progress towards a new level of security. **Setting realistic benchmarks gives you the opportunity to reward ongoing efforts by acknowledging progress** in front of peers. This will promote a sense of constructive collaboration and create an atmosphere of success even before participants reach security endpoints.

Standards and benchmarks must be ambitious enough to show recognizable progress towards a new maturity level in election security, and realistic enough that all EOs can meet them with effort.

Assess Staff and Organization Structures, Seek Feedback from Local Election Offices

Keeping in mind your state election calendar, pick a quiet post-election period to **evaluate your project staff and the mechanisms and tools** you have chosen. In addition to assessments of staff and EO work, consider structural issues. Are staff roles and responsibilities defined appropriately? Are EO advisory or work groups productive? Or would a reorganization or an infusion of new blood get them on track?

- Are staff accomplishing what they've been assigned?
- Are assignments matched to the goals of the project?
- Are EOs making progress towards a stronger security posture?
- What can be done to help EOs that are lagging?
- Are your EO steering committees or work groups functioning and constructive? How can they be re-energized? Should the mix of EOs be adjusted to create a more successful team?

As part of the evaluation process, prepare a survey to solicit feedback from EOs, assess progress and begin setting new targets. Some sample questions that you can adapt are below.

1. **Have you worked with your Security Navigator?**
2. **Do you find the advice helpful?**
3. **Do you find the Navigator has the necessary knowledge about elections?**
4. **Can you name an instance where you've changed a procedure or added a security control because of the Navigator program?**
5. **Do you feel that you, your staff and elections in your county are more secure today because of the program?**
6. **Are you satisfied with opportunities to participate and help focus the program on your security priorities?**
7. **Are there any priorities you would like to share now?**

Setting New Goals and Standards

Showing responsiveness to the concerns identified in your survey and evaluation process is critical. **The feedback received will improve procedures and help you update goals** for the coming year or draft plans for the next phase of the project. If the program has succeeded, you may be able to establish higher security standards or address security domains that budget, resource or program maturity issues had prevented you from addressing in the first year.

Communicating with Stakeholders and the Public

As with some other topics, a thorough discussion of project communications is beyond the scope of this guide because the goals and methods of each program are so disparate. We will emphasize two aspects of communications.

First, remember the need for **consistent internal communications to keep all partner agencies aware of deadlines and key issues, and apprised of progress towards benchmarks**. This could take the form of sending an email newsletter, writing individual emails or calling contacts to let them know about progress. Some potential topics include:

- New security tools, either developed in-house or available online
- Successful implementations (maybe focused on an early-adopting jurisdiction)
- Notes on the changing security environment
- Thank-yous to participants in work groups

Second, a primary goal of any security project is **deterring threats by letting troublemakers know they face strong defenses**. Therefore, public communications about project accomplishments are important. The work of your Navigator program is one facet of **the long-term, ongoing, critical effort you are all engaged in – ensuring the integrity of elections in your state**. Let the public know your elections are trustworthy, and this project is helping ensure they remain so.

Finally, we underline the importance of communicating about your successes both internally and to the public. **Giving all participants a sense of their progress and achievement will strengthen their commitment to the program, refresh their energy for reaching its targets** and motivate them to continue.

Appendix

Organizations with Resources for Security Navigator Programs

As you continue to think through building a Security Navigator program for your state, you can find a lot of helpful information at the websites of the following organizations:

- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- Center for Internet Security (CIS)
- Committee for Safe & Secure Elections (CSSE)
- Election Assistance Commission (EAC)
- National Institute of Standards and Technology (NIST)
- The Elections Group (TEG)
- Center for Technology and Civic Life (CTCL)