LEADING CYBERSECURITY CONVERSATIONS

With Your County Team

Election infrastructure faces increasingly complex cybersecurity threats, with attacks growing more sophisticated and frequent.

To protect public trust and operational effectiveness, it has never been more critical for officials across all aspects of government to engage in proactive, informed conversations. This nonpartisan guide is designed to help election officials approach those discussions with clarity, confidence and purpose by breaking down the meeting into more tangible phases: *Preparation, Execution, and Follow-Up*.

Having a robust conversation with your team about your election-related cybersecurity needs involves preparation, common ground and collaboration. To discuss cybersecurity needs, you may want to consider having not only your IT staff at the table, but also include your elected official(s), finance staff and emergency managers. Consider preparing in a way that:

> **Identifies common ground**
> **Clarifies your priorities and defines potential risk**
> **Frames cybersecurity as a shared responsibility, building cross-departmental understanding**
> **Secures buy-in by connecting technical needs to operational and budget realities**

Preparing for the Meeting

1 **Identify your objectives.** Before walking into the room, know what you want to accomplish.

Do you need approval for funding? Are you looking for technical support or interdepartmental coordination? Do you want to build a shared understanding of cyber risks to election infrastructure?

Set 1-2 clear outcomes and align your message accordingly.

2 **Understand roles early.** Since you will have a diverse audience, and each group has different concerns and decision-making authority, be sure to understand their interests and responsibilities ahead of the meeting. Consider using plain language and avoiding overly technical terms. Explain cybersecurity in terms of a shared responsibility, organizational risk reduction and resilience.

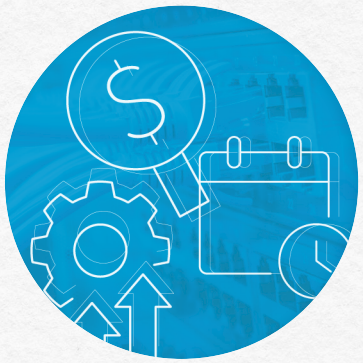
STAKEHOLDER	COMMON PRIMARY MOTIVATORS	SUGGESTED FRAMING
Elected Officials	Public trust, accountability, visible investment in secure elections	Focus on risk, cost, legal exposure and public trust.
IT Staff	Security protocols, infrastructure, technical feasibility, integrating with existing systems	Ask for help identifying specific needs and prioritizing upgrades. IT is instrumental in implementing new services.
Finance Staff	Budget constraints, costs, funding opportunities (HAVA, DHS grants), ROI	Show how cyber investment protects public trust and avoids costly breaches.
Emergency Managers	Coordination on continuity of operations, incident response	Coordinate planning for ransomware or cyber disruptions on Election Day.

3 **Know your cybersecurity needs.** Make a list of needs tied to your systems, assets and operations. Break them down into easy-to-understand categories, such as essential, want-to-have and nice-to-have. Be ready to explain the difference and how it relates to potential risk and real-world examples. Don't assume everyone in the meeting will understand cybersecurity and how it could impact election operations. Below are some examples to consider:

- **Multi-Factor Authentication (MFA):** Prevents unauthorized access to voter systems
- **Endpoint Detection & Response (EDR):** Detects threats on computers used by election staff as well as other staff in the jurisdiction
- **Encrypted, offline backup:** Ensures recovery if systems are attacked
- **Incident response plan coordination:** Enables smooth response with emergency managers

4 **Bring supporting materials.** Helpful documents might include:

- A one-page overview summarizing your current posture, key gaps, essential needs and key election dates and deadlines
- Cost estimates and potential funding opportunities, including grants, application deadlines and compliance requirements
- A timeline for implementation, including blackout windows during peak election periods
- Relevant election security best practices (CISA, MS-ISAC, CIS)



5 **Be ready to answer key questions.** Anticipate and prepare for questions like:

What's the risk if we do nothing?

What level of risk is acceptable?

Can we phase this over time?

Is there grant funding available?

How do we know the investment will work?

What coordination is needed across departments?

Can we share costs or services across departments?

What's our legal or compliance obligation?

Conducting the Meeting

1 **Set the stage: Define the purpose and establish common ground.** Start with a clear explanation of why this conversation matters and acknowledge the goals shared by all stakeholders. For example, cyber threats to local governments are increasingly sophisticated and frequent, elections are an essential service, and it's important to maintain public trust. Certain risks to elections can be mitigated by ensuring systems, data and people are protected. This conversation aims to help us understand our current situation, identify areas for improvement and prioritize the next steps we need to take.

2 **Clarify your cybersecurity needs.** Consider starting by identifying your:

- **Core election systems:** Voter registration, election management, e-pollbooks, election night reporting, etc.
- **Cyber risks or vulnerabilities:** Outdated software, phishing attacks, limited incident response capability, etc.
- **Services you already have and those you are missing:** Multi-factor authentication, endpoint protection, encrypted and offline backups, etc.

3 **Use a simple framework to guide the discussion.** Organize the conversation around a few core areas. For example, you can frame the conversation as: We're here today because protecting voter data is a shared responsibility. Our systems face real threats, and we need to align on priorities and resources.

> **Current Status:** *What protections are currently in place?*
> **Key Risks:** *Where are our biggest vulnerabilities?*
> **Priority Needs:** *What actions are most important?*
> **Resources:** *What budget, tools or expertise do we already have?*
> **Next Steps:** *What can we realistically do this quarter or year?*

4 **Frame cybersecurity as a shared responsibility.** Clearly articulate how cybersecurity is a collective effort, emphasizing the importance of individual and departmental involvement in safeguarding data and systems; it's not just about elections. Emphasize the public trust at stake, the need for proactive investment (not just reactive fixes) and the importance of teamwork across departments.

5 **Review the threat landscape.** When reviewing the cyber threat landscape, provide each participant the opportunity to share any threats or risks they are aware of. This should include discussion of the latest intelligence and alerts (from CISA, MS-ISAC, FBI, private sector vendors, etc.), emerging adversary tactics, techniques and procedures (TTPs) and recent high-profile incidents. The conversation should also cover the primary attack vectors, the cybersecurity measures currently in place to reduce exposure and any gaps or vulnerabilities that still need attention.

6 **Confirm outcomes and decisions.** Document the discussion, identify owners for key actions and set a timeline for follow-up meetings or updates.

After the Meeting

1 **Distribute meeting documentation.** Send concise, clear notes, highlighting deadlines, deliverables and responsible parties.

2 **Sustain the dialogue.** Keep the conversation going:

- Schedule regular meetings: Transition from a one-off meeting to a consistent schedule (e.g., monthly) to maintain momentum and foster an ongoing dialogue about cybersecurity services.
- Use collaborative tools (Google Docs, Teams, Slack channels, shared project boards) so updates and ideas happen in real time.

3 **End the conversation with a call to action**, similar to: *"Grateful for the energy and ideas shared today. Together, we're not just checking boxes, we are building resilience and protecting democracy. Let's keep pushing forward."*

Protecting elections from cyber threats isn't a solo effort; it's a team sport.

By establishing common ground, identifying clear objectives, understanding each person's role and connecting technical needs to real-world operations, you set the stage for productive conversations. In the meeting, use a simple framework to guide the discussion, frame cybersecurity as a shared responsibility and confirm clear outcomes. Afterward, follow through—document the results, share them with your team and keep the momentum alive. Each step you take strengthens your network of support and builds resilience, helping ensure your systems—and your elections—remain secure.

ELECTION SECURITY RESEARCH PROJECT

A joint effort between

CENTER FOR TECH AND CIVIC LIFE

PLEJ PARTNERSHIP FOR LARGE ELECTION JURISDICTIONS

The Elections Group

and a **COHORT OF ELECTION SECURITY EXPERTS**