Leading Cybersecurity Conversations with External Partners

ELECTION SECURITY Exchange

Election infrastructure faces increasingly complex cybersecurity threats, and much of the technology and services that support it are delivered by external partners: contract IT providers, managed service providers (MSPs), and elections technology vendors. These relationships introduce both opportunity and risk. Understanding how to lead productive cybersecurity conversations with these partners and how to hold them accountable through contracts, service-level agreements (SLAs) for monitoring and system management, and incident response and continuity planning is essential to protecting election operations. This guide helps election officials approach those conversations with clarity, confidence, and purpose, organized into three phases: preparing for the meeting, conducting the meeting, and following up afterward.

Having a robust conversation with your external partners about cybersecurity requires preparation, clear expectations, and mutual accountability. Before meeting with a contract IT firm, a managed service provider, or an elections technology vendor, consider preparing in a way that:

- Establishes clear contractual expectations and cybersecurity obligations,
- Defines service level agreements and measurable performance standards,
- Clarifies incident response roles, duties, and notification timelines, and
- Aligns vendor capabilities with your jurisdiction's security requirements and election timelines.

Preparing for the Meeting

1. Identify Your Objectives

Before meeting with an external partner, be clear about what you want to accomplish.

- Are you reviewing or renegotiating an existing contract or SLA?
- Are you evaluating whether the vendor meets your cybersecurity requirements?
- Do you need to establish or clarify incident response duties, notification timelines, or escalation contacts?

Set 1–2 clear outcomes and bring any existing contract documents, SLA language, or prior incident reports to the meeting.

2. Understand Roles Early.

Different external partner types have different priorities and decision-making structures. Understanding those ahead of time allows you to frame your requirements in terms they will act on. The stakeholder table below provides a starting point. Confirm who from the partner organization will be present—technical staff, account managers, or legal representatives—and tailor your materials accordingly.

Stakeholder	Common Primary Motivators	Framing Examples
Contract IT Provider	Contract scope, billable services, liability limits, renewal opportunities	Anchor the conversation in the security standards already in the contract, compliance obligations both parties share, and the remediation path if performance falls short.
Managed Service Provider (MSP)	Scalable service delivery, SLA metrics, and minimizing disruption to managed environments	Define response time requirements, uptime guarantees, patch management duties, and incident notification windows in the SLA
Elections Technology Vendor	Certification compliance, product roadmap, support contracts, limiting scope creep	Emphasize independent verification (U.S. Election Assistance Commission (EAC) certification for voting systems, the Center for Internet Security's (CIS) Rapid Architecture-Based Enterprise Technology Verification (RABET-V) for non-voting election technology), security patch timelines, data access controls, and breach notification duties under the contract
Legal / Procurement	Risk transfer, indemnification, regulatory compliance, contract enforceability	Connect cybersecurity contract terms to liability exposure, insurance requirements, and regulatory obligations informed by federal, state, and industry security advisories, as well as state data breach laws.

3. Know Your Contract and Security Requirements.

Review your current contracts and SLAs before the meeting. Identify what cybersecurity requirements are already in place and where there are gaps. Categorize them by need such as, required, strongly recommended, and aspirational. Be ready to explain how each connects to real operational risk. Below are examples of key areas to cover:

- **Cybersecurity contract terms** – specific security standards according to state and/or federal requirements (e.g., National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), CIS Controls), public records cooperation provisions (vendor notification of records requests, support for exemption claims, designation of records as critical infrastructure information where applicable), data handling and access provisions, non-disclosure requirements, breach notification timelines, specifics of their vulnerability disclosure program (VDP), and indemnification clauses
- **Service Level Agreements (SLAs)** – uptime guarantees, response times for security incidents, patch and update deployment windows, expanded support during key election periods, and performance reporting frequency
- **Incident Response Capabilities and Duties** – who leads detection and triage, mandatory notification timelines (e.g., 24 or 72 hours), forensic preservation requirements, partner escalation contacts, and coordination with law enforcement, insurance providers, Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing & Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC)
- **Access Controls and Supply Chain Security** – remote access restrictions, multi-factor authentication requirements for vendor personnel, subcontractor disclosure, and machine-readable hardware and software bill of materials (HBOM/SBOM) delivered with each release and monitored against known vulnerability databases throughout the contract term

4. Bring Supporting Materials.

Helpful documents might include:

- A one-page summary of current contract cybersecurity requirements, known gaps, and priority issues to resolve
- Proposed contract language or SLA terms for cybersecurity obligations, including specific metrics, notification windows, and remediation deadlines
- An election calendar showing blackout windows, peak periods, and critical deadlines when system changes or maintenance are restricted
- Relevant security frameworks and guidance (NIST CSF, NIST SP 800-53, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001 and 27002, CISA election security resources, CISA Secure by Design principles, MS-ISAC/EI-ISAC, CIS Controls, EAC guidelines, guidelines and best practices highlighted by the Election Security Exchange) to support your requirements

5. Plan for Limited Contract Language.

Not every jurisdiction has the contract authority, procurement support, or vendor alternatives to demand sweeping changes. If you are mid-cycle on a multi-year agreement, working with a sole-source vendor, or operating without dedicated legal or procurement staff, focus the conversation on what is achievable:

- Side letters or memoranda of understanding (MOUs) that document specific cybersecurity commitments without reopening the underlying contract
- Joint incident response playbooks and tabletop participation, which often do not require contract amendments
- Pooled leverage through your state association of election officials, chief election official's office, or MS/EI-ISAC, which can raise vendor-wide issues on behalf of multiple jurisdictions
- Timing major asks for the Request for Proposals (RFP) or renewal window, while using the current cycle to document gaps and build the evidence base

Limited leverage doesn't mean you should skip the conversation. Documented gaps, even unresolved ones, create the record that supports stronger terms at renewal.

6. Be Ready to Ask and Answer Key Questions.

Bring a written list so nothing important gets skipped. Examples:

- **What happens if you fail** to meet an SLA requirement during an election period?
- **Who on your team is responsible** for detecting and reporting a security incident, and within what timeframe?
- **How do you handle subcontractors** or third parties who access our systems?
- **What background check, credential verification, and access revocation processes** do you have in place for your own personnel who access our systems, and how quickly can you revoke access if a staff member leaves or is terminated?
- **What security certifications or audits have you completed** in the past 12 months (e.g., System and Organization Controls 2 (SOC 2), penetration testing)?
- **Can you provide evidence that required patches** or updates were applied within the contractually required window?
- **What notification process do you follow** if one of your other clients suffers a breach that could affect shared infrastructure?
- **How are contract modifications handled** if new cybersecurity requirements emerge during the contract term?
- **What are your retention and termination rights** if the vendor fails to meet security obligations?
- **What is our legal or regulatory exposure** if this vendor experiences a breach affecting voter registration data or PII collected during registration?
- **Beyond point-in-time tests, how do you demonstrate organizational security maturity** over time, and what independent assessments (RABET-V, SOC 2 Type II, third-party penetration testing programs) can you provide evidence of?
- **How will you handle records you provide to us** if we receive a public records request that touches your security documentation? Will you notify us of any third-party request you receive that names our jurisdiction, and will you support our application of any applicable exemptions, including the PCII Program where appropriate?
- **What are your business continuity and disaster recovery capabilities** if your organization experiences a major disruption? If you become unavailable during an active election period, what is the exit path, and how quickly could we transition to a backup provider?

7. Plan for Public Records Risks.

Sensitive vendor information you receive (incident reports, vulnerability assessments, HBOM/SBOMs, penetration test results, security architectures, system logs) can become part of the public record once it is held by your agency. State public records laws vary widely. Most states have some form of critical infrastructure, security plan, or cybersecurity exemption, and a small number have explicit election security exemptions, but coverage is uneven, and the burden of proof typically falls on the agency withholding the record.

Before the meeting, do three things:

- **Review your state's public records law with counsel** and confirm which exemptions could apply to vendor security records (critical infrastructure, security plans, cybersecurity, infrastructure protection, trade secrets, or law enforcement records). Confirm whether any election-specific exemption exists.
- **Confirm whether your jurisdiction is eligible and interested in using the federal Protected Critical Infrastructure Information (PCII) Program.** PCII validated by CISA is exempt from Freedom of Information Act (FOIA) and "similar State and local disclosure laws" under 6 U.S.C. §§ 131 et seq. and 6 CFR Part 29. PCII can be a route for the most sensitive vendor-provided records, though it requires designated PCII Officers and authorized users.
- **Coordinate with your legal team to understand how your agency approaches record retention** and what materials are appropriate to review without taking custody. In many jurisdictions, whether an agency holds a record can influence how it is treated under public disclosure laws, so it is helpful to clarify your internal practices before meeting with a vendor. For sensitive materials such as vulnerability assessments, penetration test results, or detailed system architectures, you may determine that reviewing them on the vendor's premises or through controlled access meets your oversight needs while allowing the vendor to retain custody.

Coordinate with your state association of election officials, chief election official's office, or attorney general before adopting practices that diverge from how peer jurisdictions handle these records.

Conducting the Meeting

1. Set the Stage: Establish the Purpose and Ground Rules.

Open by framing the meeting as a collaborative but accountability-focused conversation. Make clear that the purpose is to verify, align, and document cybersecurity expectations—not to assign blame. For example: "We rely on your services to support secure, resilient elections. This conversation is about making sure our contract and our working relationship reflect the cybersecurity standards that our community and the law expect. We want to leave today with clear, documented commitments we can both stand behind."

2. Review Contract Terms and SLA Performance.

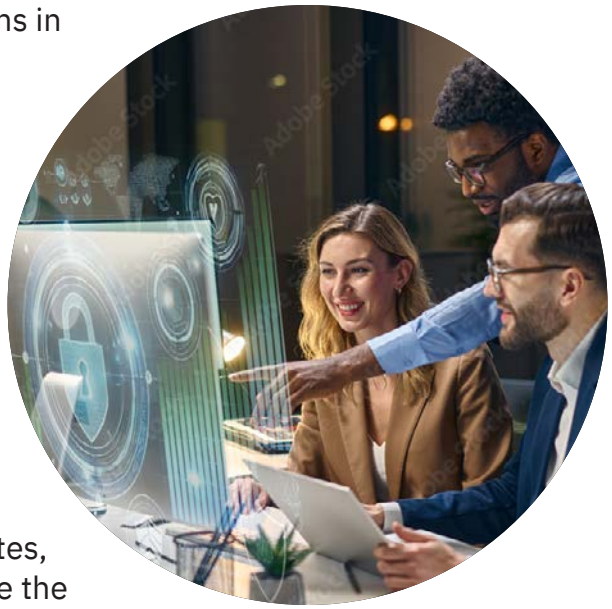
Walk through the current contract and SLA side by side. For each cybersecurity requirement, confirm whether it is being met, partially met, or not yet addressed. Things to consider asking about:

- Current security controls and how they map to contractual requirements
- Any known gaps, open vulnerabilities, or prior incidents relevant to your environment
- Their incident response process and the specific individuals responsible for detection, containment, and your notification

3. Use a Structured Framework to Drive the Discussion.

Organize the conversation around five core areas that apply directly to external partner relationships. For example, you can frame the agenda as: "We're here to make sure our partnership meets the security standards elections require. Let's review where we stand and what needs to be formalized."

- **Contract Status:** Are all required cybersecurity terms in place and understood by both parties?
- **SLA Performance:** Are uptime, response time, and patch management obligations being met? Where are the gaps?
- **Incident Response Readiness:** Do both parties understand their roles, notification duties, and escalation contacts in the event of a breach or disruption?
- **Unresolved Gaps:** What security obligations remain unaddressed, and what is the remediation timeline?
- **Next Steps:** What contract amendments, SLA updates, or operational changes need to be formalized before the next election cycle?



4. Address Incident Response Duties Explicitly.

One of the most critical—and often unresolved—areas in vendor relationships is incident response. Be direct. Ask the partner to confirm: who on their team is the primary security contact, what their detection and notification process looks like, how quickly they can isolate affected systems, and what documentation they will provide following an incident. It's important to make sure they understand that election blackout windows require accelerated response timelines and that notification delays are not acceptable. These are the types of specifics that you can discuss with your attorney to capture in contract language or an addendum.

5. Review the Threat Landscape and Vendor Exposure.

Ask the partner to share how they stay current with the threat landscape relevant to your environment. Topics to consider: how they have adjusted to AI-enabled threats such as jurisdiction-tailored phishing, voice and image impersonation, and automated reconnaissance against staff and partners. With AI-leveraged attacks, your window for responding may be compressed as attackers and defenders move at machine speed. AI is not a new category of threat, but it lowers the cost and skill required to execute familiar threats, and it changes the timelines vendors need to meet.

How they consume threat intelligence from federal, state, and industry security advisories, including CISA and the MS/EI-ISAC, and sector-specific advisories; how they test and validate their own defenses; and how they have responded to recent high-profile incidents affecting similar organizations. Discussing whether they have experienced any breaches or near-misses involving election clients, and what changes resulted also helps you assess their actual security maturity—not just their contractual commitments.

Another important topic is understanding how they verify the identity of out-of-band requests. For example, if someone claiming to be from your office calls asking for emergency access. AI-enabled voice and image impersonation make this a realistic attack vector against your vendor contacts, not just your own staff.

6. Confirm Outcomes and Document Commitments.

Before closing the meeting, summarize every commitment made, verbally or in writing, and assign a named owner and deadline to each. If changes are appropriate, consult with legal to counsel to confirm which items require formal contract amendments, which can be addressed through an SLA addendum, and which will be tracked through ongoing performance reporting. Make clear that unresolved gaps will be documented and revisited at a defined follow-up date.

After the Meeting

1. Distribute a Written Summary of Commitments.

Within 48 hours, send the partner a written summary of what was agreed, what was left open, and what the next steps are. This creates a record that can inform contract amendments and serves as the basis for accountability if commitments are not met. Include: each open cybersecurity item and its agreed resolution or remediation deadline; any SLA terms that need to be revised or added; named individuals responsible for each action; and the date of the next scheduled review. Treat the summary as a record subject to your state's public records law. Mark it consistent with your records protection scheme, store it accordingly, and avoid including specific vulnerability details or system configuration information that is not necessary for the operational purpose of the summary. Where appropriate, describe gaps and remediation deadlines in functional terms rather than reproducing technical detail from the vendor's documentation.

2. Pursue Contract Amendments and SLA Updates.

Do not let verbal commitments substitute for written contract terms. Work with your legal or procurement team to formalize agreed cybersecurity requirements as amendments or addenda to the existing contract. Priority items to consider capturing in writing include:

- **Breach notification timelines** (e.g., notify the jurisdiction within 24 hours of any confirmed or suspected incident affecting election systems)
- **Specific security controls required of vendor personnel**, including Multi-Factor Authentication (MFA), background check requirements, and restrictions on remote access during election periods
- **Records-handling provisions that address public records risk**, including: vendor notification when the jurisdiction receives a records request implicating vendor materials, vendor cooperation in identifying records eligible for exemption, marking of sensitive deliverables (vulnerability assessments, penetration test results, HBOM/SBOMs, security architectures) consistent with the jurisdiction's records protection scheme, and a clear understanding of what the vendor retains versus what is delivered to the jurisdiction
- **Indemnification language that addresses who bears the cost of forensic investigation, system restoration, and public communications** in the event that a vendor-side failure causes or contributes to an incident affecting your jurisdiction.

3. Maintain Ongoing Oversight.

Vendor cybersecurity is not a one-time conversation. Schedule recurring security reviews on a defined cadence (quarterly for high-risk systems, semi-annually at minimum) to assess SLA performance, review any incidents or near-misses, and update contract terms as the threat landscape evolves. Make contract renewal contingent on continued adherence, not just initial certification. Before each election cycle, confirm in writing that all security requirements are in place and that incident response contacts are current. Keep your internal team, legal counsel, and emergency managers informed of vendor performance so they can act quickly if a partner falls short. If you share a vendor with a neighboring jurisdiction, you can also coordinate with peer offices so that a single vendor failure does not cascade into simultaneous disruption across multiple election operations without a coordinated response.

Conclusion

Managing cybersecurity across external partners requires preparation, precision, and persistence. By understanding what each vendor type cares about, reviewing contracts and SLAs before you meet, and pushing for specific incident response commitments, you set the conditions for genuine accountability, not just good intentions. In the meeting, use a structured framework to work through contract status, SLA performance, and incident response readiness. Afterward, follow through: put agreements in writing, formalize amendments with your legal team, and build a regular review cadence into your vendor relationships. Election infrastructure depends on partners who can meet the moment. You can make sure those expectations are clear, documented, and enforced.