Center for Internet Security®
Creating Confidence in the Connected World.™

Guide to Election Technology Procurements

Mike Garcia
Marci Andino

Release 1.1

CONTENTS

CHAPTER

ONE

THE CIS GUIDE TO ELECTION TECHNOLOGY PROCUREMENTS

Computer hardware, software, and services are essential for election operations. Many of the hardware, software, and services that underpin our elections—from voter registration and election management systems to pollbooks and vote capture devices—are procured from private vendors. Even simple public-facing websites may be procured. The security of each of these systems may have consequences on election administration. The industry partners from which information technology (IT) is procured play a critical role in managing the security risks inherent in elections. Understanding and properly managing security expectations in the procurement process can have a substantial impact on the success of the election process.

1.1 About this Guide

The Center for Internet Security®[1] (CIS®) developed this guide benefiting from input and feedback from state and local government, federal government, academic, and commercial stakeholders. The goal is to impact and improve the security of election infrastructure by providing a set of specific security best practices for IT procurements in elections that complement CIS's Essential Guide to Election Security[2], and other CIS best practices work.

This is an updated version of the original guide, released in 2019, which is available here.

1.2 Navigating the Guide

Use this document like a normal PDF. Some features, like worksheet downloads, are only available via the online version, which you can always access here: https://election-procurement.docs.cisecurity.org.

If you like working off the PDF, we still recommend downloading it anew from the online version so that you always have the most up-to-date content.

[1] https://www.cisecurity.org

[2] https://essentialguide.docs.cisecurity.org/en/latest/README.html

1.3 Contents

This guide contains:

- A *brief summary* (page 3) of IT procurements in elections.
- A *summary* (page 45) of the best practices and model language found in this guide.
- A set of *best practices* (page 4) that election administrators can use in their procurements.
- *Model procurement language* (page 39) that election officials can use to communicate their security priorities, better understand vendor security procedures, and facilitate a more precise cybersecurity dialogue with the private sector. *NOTE: This section is still in development and we need your help! Submit model language to use and we'll post it here.*
- An *overview of security risk* (page 40) in election technology procurement, including information on assessing and managing security risk in election systems.
- A description of a typical *IT product and services lifecycle* (page 43), describing product purchase and support, system development and maintenance (including updates and patching), and the services lifecycle.
- A more detailed *primer on the IT Procurement Process* (page 47), with descriptions of the typical IT procurement processes applicable across a range of organizations.
- *Additional resources* (page 56) for procurement and related information with links to procurement opportunities, training, and other useful information related to election procurement.

CHAPTER

TWO

A BRIEF SUMMARY OF IT PROCUREMENT IN ELECTIONS

To successfully execute a procurement, election administrators should understand a few basic concepts. Learn more about these processes in the latter sections of this guide, including on *security risk* (page 40), the *IT product and services lifecycle* (page 43), and a more detailed *primer on the IT Procurement Process* (page 47).

2.1 Protecting Confidential Security Information

Cybersecurity often implicates a tradeoff between confidentiality in security techniques and maximizing transparency of government activities. Many vendors are hesitant to share security information that, if disclosed, could benefit attackers or industry competitors. Yet government offices have a fundamental obligation to share information with the public.

Election offices should consult with their legal and procurement teams to better understand what information can be held closely, and what must be released. During procurements, this determination should be made clear to potential proposers as well as how to mark information as proprietary and confidential. If you are unable to protect vendor proprietary and confidential information from disclosure, you should expect to receive less detailed information from proposers.

2.2 The Players

Typically, election officials and their teams, procurement teams, and IT teams all have a role to play in election IT procurements. In many jurisdictions, poll workers and the public are also involved, and elected officials often have a critical role in setting priorities and budgets. To the extent possible, this is good for transparency and may also provide opportunities to educate others about your approach to security.

Election officials are the customer, and procurement and IT teams are there to help the election officials achieve their goals. While these different entities may be in the same organization, they may not always see the problem the same way. Together, by focusing on their respective roles and communicating well, these teams can complete efficient and effective procurements.

CHAPTER

THREE

BEST PRACTICES FOR CYBERSECURITY IN ELECTION IT PROCUREMENT

This guide contains a set of best practices that election officials can use in their procurements to improve security outcomes. The best practices are intended to generate responses from potential vendors that can help election officials make informed decisions.

For each of the best practices, we provide a few classifications to help understand and prioritize their use. Each best practice can fall under multiple items within each category. For instance, a best practice may address hardware, software, services, or cloud-based IT, or it may apply to some combination of those. While we also provide descriptions of good and not-so-good responses, for all of this guidance, it's up to the officials to know if a proposer's response meets their needs.

The following table provides the format of each best practice and includes:

- A description of the best practice, numbered sequentially beginning with #1
- A classification of whether the best practice applies to people, processes, or technology
- Suggested applicability to all or only operational systems
- The type of IT to which the recommendation applies
- Suggested language you can put in your procurement documents
- A description of a good response or activity
- A description of a bad response or activity
- Some additional tips, if any
- Helpful references and links, if any

3.1 Viewing the Best Practices

The best practices are listed in individual tables below. In addition, you can download an Excel file by going to the online version of this guide. If you return to this section, you'll get an option to download the Excel file.

Go directly to this section of the online version here: https://election-procurement.docs.cisecurity.org/en/latest/bp_tables#viewing-the-best-practices.

3.2 Best Practices

Table 1: Best Practice #1: Individual Qualifications

Number	Name	Category	Applicability	IT type
1	Qualifications and experience of individuals proposed for work.	People	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide qualifications and experience of all proposed personnel, including subcontractors. In addition to basic qualifications (e.g., certifications obtained), include descriptions of experience in the area of elections or cybersecurity, or both. Where applicable, provide any specific knowledge and experience with state and local policies, architecture, and related aspects of the proposed work.			
Good Responses	While combined experience of a team is valuable, it's not always sufficient. To provide confidence that they understand the complexities of election infrastructure, as well as modern cybersecurity principles and practices, at least some personnel with significant time on the project will have experience with both elections and cybersecurity.			
Bad Responses	Listing key personnel without specific names or qualifications. Lack of personnel with direct cybersecurity experience. For those listed, years of experience are provided as a qualification but with a lack of specifics on skills or role in security.			
Tips	Expect demonstrated experience doing exact work that has similar cyber challenges (preferably within elections domain).			
	Proposed personnel should have a number of years of experience appropriate to their proposed responsibilities as well as relevant degrees and certifications. (Note, however, that certifications can be obtained without demonstrating hands-on experience and should not, on their own, constitute qualification.)			
	Look at the ratio of knowledge and experience in-house vs. with subcontractors. It is preferred to have qualifications in-house.			
	A team of resources who have worked together on relevant projects are preferable to one that has not worked together on prior engagements. The sum of the whole may be greater than the parts.			

Table 2: Best Practice #2: Past Performance

Number	Name	Category	Applicability	IT type
2	Demonstrated past performance performing proposed work. Includes awareness of, and experience adhering to, applicable certifications and legal and regulatory requirements.	People	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide references, including contact information, for past performance with comparable-sized customers and, in particular, in the election environment. Ideally, these will be public sector election organizations at a state or local level. Contact information should include those responsible for the security portion of the project. Include work in a similar legal and regulatory environment and in obtaining any relevant certifications.			
Good Responses	The contacts provided match the prior engagements that were similar to your organization's needed approach. Ideally you will recognize at least some of the organizations, if not the names themselves. The references should be true cybersecurity people, or as close to one as exists in the client's organization.			
	The responder demonstrates an understanding of the legal and regulatory regimes applicable to the contract and other work in which the proposer is involved, including knowledge of local and state requirements as well as any applicable federal regulations.			
Bad Responses	Generic statements of experience in the field or related field, but not citing any examples.			
	Generic statement that legal and regulatory requirements will be met during the work.			
Tips	Require comprehensive disclosure of projects of similar scope and complexity by the proposer within the past three years, whether they are included as a reference project or not. You want information on challenging project engagements as well as successful projects when you are considering past performance.			
	Multiple references are a must. They can be from the recent past but should also include some more recent ones. Generally, references that are older than three years can be considered not useful. Evaluate references with points of contact to validate past performance to ensure that the proposer does quality work and has appropriate focus and experience with security requirements expected for this work.			
	If the proposer indicates the contact is the only allowable reference (some organizations may only allow a procurement official to field reference calls), explain to the procurement official that you are checking on technical cybersecurity credentials and would like to speak with a technical representative.			
	In addition to solicitations in which the proposer was selected, consider requesting information on similar solicitations pursued when the proposer was not selected.			
References and Links	DHS Election Infrastructure Funding Considerations[3]			
	Brennan Center for Justice, A Procurement Guide for Better Election Cybersecurity[4]			

Table 3: Best Practice #3: Personnel Policies

Number	Name	Category	Applicability	IT type
3	Proposer personnel policies regarding hiring and conduct standards, including background check, citizenship, and visa requirements.	People	All systems	Hardware, Software, Services, Cloud
Suggested Language	Describe your company process for background checks and security training of those who will be working on the project. Individuals working under this contract must have the same or equivalent background screening and IT security training as government employees.			
Good Responses	Detailed descriptions of the types of vetting that occurs: criminal, financial, federal, etc.			
Bad Responses	Statements that background checks are conducted with no additional details on the type or extent of vetting.			
Tips	All personnel that work on the contract should have at least a national agency check and should be U.S. citizens. If some employees are not U.S. citizens, proposer should detail risk management procedures and provide results of background checks on those staff members or contractors.			
	Proposer should provide their processes to ensure that malicious employees cannot compromise security (e.g., limited access and two-person rule for most critical jobs or functions, with appropriate access monitoring in place).			
References and Links	National Agency Check Criminal History[5]			

[3] https://www.dhs.gov/sites/default/files/publications/Election%20Infrastructure%20Security%20Funding%20Considerations%20Final_0.pdf

[4] https://www.brennancenter.org/publication/procurement-guide-better-election-cybersecurity

[5] https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history

Table 4: Best Practice #4: Work Location

Number	Name	Category	Applicability	IT type
4	Proposer location(s) where work will be performed and equipment supported as well as administrative and facility security at the location(s).	People	All systems	Services
Suggested Language	Provide all work locations and descriptions of physical and logical security requirements, handling of sensitive materials, and emergency and disaster backup provisions. Describe how you will manage various work locations from the perspective of election security. This includes adherence to government requirements that all work and data storage be maintained in the United States, as applicable.			
Good Responses	Describes any work locations and, if multiple, the work performed at each. Facility security descriptions do not need to provide precise measures but should state basic approaches such as entry door badge requirements and presence of security systems.			
Bad Responses	No defined policies. Not responsive to stated requirements (such as if, in the RFP, you state that personnel must/must not work in specific locations).			
	Failure to specify the locations at which the proposer anticipates work. Vague statements about commitment to security and maintaining properly secure facilities.			
Tips	Care should be exercised in using out-of-country contractors or contractor personnel who are not U.S. citizens. They are not inherently bad, but the government needs to be aware that there are risks that will be more difficult to quantify and control. Moreover, some countries may not be acceptable work locations and others may require special controls. Citizenship requirements may be set by the state or locality and may reflect the sensitivity of the products or services being procured.			
	For most specialized election products and services, it is reasonable to expect development to occur in the United States by U.S. citizens. Generalized hardware and software will often have global supply chains, but election officials may want to have the final product developed by a U.S.-based company or, at minimum, one with an established U.S. presence and reputation.			

Table 5: Best Practice #5: Training Procedures

Number	Name	Category	Applicability	IT type
5	Training procedures for the proposer.	People	All systems	Services
Suggested Language	Describe security training requirements for personnel. Include descriptions of different training for different types of personnel (e.g., system administrators, developers, administrative). Confirm that these same requirements also apply to any subcontractors.			
Good Responses	All employees undergo security awareness training, and those in sensitive and critical security positions have more in- depth training (e.g., threat identification and risk identification). Proposer should describe training content, frequency, and testing approaches.			
Bad Responses	Basic statements that employees undergo security training without further description of the type of training. Failure to describe specialized training for critical positions. Indications that suggest security training is ad hoc or otherwise lacks a systematic approach.			
Tips	Security training from a reputable provider is most common. Training provided by internal personnel is acceptable if the person is sufficiently qualified.			
	Look specifically for mentions of phishing, email, and browsers in training curriculum.			
	If software development and customization will be provided under the project, request specific information on secure coding and development curriculum.			
	Look for monitoring and reporting of training activities – e.g., 100% of all proposer personnel have completed required cybersecurity and awareness training.			

Table 6: Best Practice #6: Ownership

Number	Name	Category	Applicability	IT type
6	Company ownership, board members, and stakeholders.	People	All systems	Hardware, Software, Services, Cloud
Suggested Language	Disclose all countries in which your organization operates. Describe the corporate structure and ownership (e.g., publicly traded corporation, privately held partnership, nonprofit). Disclose all board members or any entity with more than 10% ownership in the organization. Also, disclose any ownership in your company by non-U.S. persons or entities, regardless of ownership percentage.			
Good Responses	Companies with foreign operations are not necessarily a problem but should be disclosed and disclosures researched for accuracy. Foreign ownership is not in itself a problem; however, it should be fully disclosed and you may want to put restrictions on certain countries.			
Bad Responses	Failure to fully disclose foreign activities or interests.			
Tips	At minimum, you should ensure that the organization does not come from a country with sanctions against doing business in the United States or have investors that are restricted, such as under the Committee for Foreign Investment in the United States (CFIUS).			
	Regardless of percentage of ownership, look for multiple foreign interests that may add up to a significant stake.			
	Include a clause in your contract requiring notification of any ownership changes to the election official.			
References and Links	CFIUS homepage[6]			

[6] https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

Table 7: Best Practice #7: Key Personnel

Number	Name	Category	Applicability	IT type
7	Proposer process for identifying and approving changes of key personnel who perform most critical management and technical functions.	People	All systems	Services
Suggested Language	Describe the review process for key personnel that perform critical management and technical functions. Also identify the timing of notification to the government when a change occurs and the plan for replacing those key personnel.			
Good Responses	Describes thorough vetting procedures as well as technical reviews. Indicates that the government will have the opportunity to review key personnel. With regard to contractor changes in key personnel, provides a sufficient notice period, typically at least 15 business days before the change. The replacement plan should indicate government review and approval and minimize any gap between personnel.			
Bad Responses	States only that reviews will occur in an efficient manner and that replacements will meet required qualifications.			
Tips	The government may choose to define what constitutes a “key person.” Alternatively, the government can request that the contractor define their criteria for “key persons” and the specific roles that they are proposing be key.			
	Government should retain the right to refuse reassignment of a resource that remains employed by the contractor.			

Table 8: Best Practice #8: Access to Sensitive Systems

Number	Name	Category	Applicability	IT type
8	Proposer authorization procedures for personnel with access to sensitive information and systems.	People	Operational Systems	Services
Suggested Language	Define sensitive functions and sensitive positions, and describe how individuals involved in sensitive functions and with access to sensitive information are trained and tested for knowledge and job performance. Also describe your process for how access to sensitive functions relates to an individual’s assignment as key personnel.			
Good Responses	Proposer clearly defines what constitutes a sensitive function and the related roles that are therefore considered sensitive positions. Personnel involved in sensitive functions should be trained and regularly tested (certified) for knowledge and job performance. Identification of specific personnel authorized to access sensitive information and systems as well as how and when that access will be revoked.			
Bad Responses	Blanket statements of appropriate training or assertions that all personnel have substantial training, failing to acknowledge that certain positions require greater levels of training than others.			
Tips	Look for proposers to identify administrator functions and who has access to those functions.			
	Look for references to new hire and termination checklists that are completed for each new employee and each terminated employee.			

Table 9: Best Practice #9: Subcontractors

Number	Name	Category	Applicability	IT type
9	Proposer policies and practices for subcontractor personnel.	People	All systems	Hardware, Software, Services
Suggested Language	If subcontractors will be used under this procurement, provide details on each subcontractor and the parts of the project in which they will be involved. The government should preapprove all subcontractors. Describe your process for selection and management of subcontractors, including how subcontractors are evaluated on an ongoing basis for meeting security requirements. Describe what information subcontractors will be allowed to access and how you will monitor their activities.			
Good Responses	Subcontracting plans are complete and clearly define the tasks completed under a subcontract. Details are provided for how the subcontractors are vetted, selected, and managed.			
Bad Responses	Plans to use subcontractors are incomplete or undefined. There is no evidence the subcontractors are vetted for security controls.			
Tips	Most procurement offices will have specific requirements around subcontractor use and how requirements for the prime contractor apply to subcontractors. From a security perspective, it's important to ensure that all security requirements also apply to subcontractors—including those involving the security of the subcontractors' internal operations.			
	Background check requirements should always apply to subcontractors.			
	Monitoring of contractors and logging of events should have regular reporting, with sample reports available to the government.			

Table 10: Best Practice #10: Cybersecurity Risk Management

Number	Name	Category	Applicability	IT type
10	Proposer's regular process for identifying and remediating cyber risks, with particular focus on components and information that are critical for mission success and increased attention to these elements.	Process	All systems	Hardware, Software, Services
Suggested Language	Describe your processes for identifying specific cybersecurity risks and mitigating them in the election environment, and how the implementation of the mitigation processes will increase the likelihood of success on the current proposal. Be specific and provide specific examples of how this process has been successful in both confirming proper implementation and identifying needed changes. Include lab testing and third-party testing you regularly employ.			
Good Responses	Includes identification of specific types of risks and the specific actions that were taken to mitigate them. These descriptions should be of a moderate to highly technical nature, referring to specific types of threats or attack vectors, specific port configurations, or the like. The proposer should be able to reference past experience and document their repeatable processes.			
Bad Responses	Provides general statements about client satisfaction or periods of uptime without a known incident. Refers back to the list of engagements without providing specific examples of risk mitigated.			
Tips	A good response may not refer to a specific contract so it doesn't reveal a particular client, but should still be able to provide substantial information on approaches.			
	It's OK for a response to be understandable by a nontechnical reader, but it should give the clear impression that they understand the approach in a technical sense as well.			
	Ideally there should be process alignment with the CIS Critical Security Controls, National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), ISO 27000, or another standard risk management framework.			
References and Links	CIS Critical Security Controls[7]			
	NIST Cybersecurity Framework[8]			
	ISO 27000 family[9]			

[7] https://www.cisecurity.org/controls
[8] https://www.nist.gov/cyberframework
[9] https://www.iso.org/isoiec-27001-information-security.html

Table 11: Best Practice #11: Incident Response

Number	Name	Category	Applicability	IT type
11	Security processes that include incident handling, recovery, and contingency arrangements to ensure availability. Includes incident response, such as when and how the government will be notified in the event of an incident.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide a description of processes you use for testing, patching, and anomaly handling.			
	Define or provide documentation on incident handling, recovery, and contingency processes, including communication plans, backup procedures, and process for operational data availability. This should also include items such as log and audit, log analysis and assessment, and forensics capabilities.			
	Define what constitutes an incident and any levels of severity. Include procedures for notifying the government in the event of incidents of each level of severity, to include responsibilities and liability. Additionally, provide a communication plan for handling an incident.			
	If you have cybersecurity insurance, provide proof of coverage and describe any relevant details of the policy.			
	[If the government has a security incident and event management (SIEM) system:] Are you capable and willing to provide logs in to the SIEM used by the government?			
Good Responses	The incident handling process covers all major phases, through recovery and follow-up activities. Demonstrates the proposer's ability to adequately respond to a variety of incidents. The best responses will include a thorough description of when and how the government will be informed of incidents for a given severity of incident. If asked, the proposer should be able to provide logs into the SIEM.			
Bad Responses	Does not clearly identify all phases of incident handling. Procedures are general. The proposer demonstrates no experience or competency in handling incidents.			
Tips	The communication plan should demonstrate preparation for public communications regarding incidents and breaches (e.g., holding statements, qualified individuals with experience in incident response and media, messaging management). Consider the Belfer Center's Incident Communications Plan template for an example of how to construct a good plan.			
	If you are operating a SIEM, make it clear to the proposer that even if they submit logs to you, they still maintain responsibility for detecting and addressing incidents.			
References and Links	Belfer Center Election Cyber Incident Communications Coordination Guide[10]			

[10] https://www.belfercenter.org/publication/election-cyber-incident-communications-coordination-guide

Table 12: Best Practice #12: Transition Planning

Number	Name	Category	Applicability	IT type
12	Transition plan for the end of the contract.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide a contract transition plan for the end of the contract.			
Good Responses	Specifies how transition will occur, including status and planning documents that will be provided. Defines the time for these documents to be provided. The plan should cover data, transitioning administrative rights, and other critical services, and the approach to maintaining security throughout the transition. Lessons learned should be documented.			
Bad Responses	Provides only remediation for its own performance or rationale to continue services.			
Tips	If you have specific requirements for how data or systems should be handled in the termination of a contract, consider adding those to the language.			
	Transition plan should clearly state contractor's obligations during transition (e.g., side-by-side monitoring and operational management of systems with transition target; training documentation; change management database handoff; knowledge base handoff).			
	Transition plan could include readiness assessments during the transition (initial contractor assessing any perceived gaps in the transition target's capabilities and knowledge plus transition target's assessment of their readiness to assume responsibilities).			

Table 13: Best Practice #13: Cybersecurity Responsibilities

Number	Name	Category	Applicability	IT type
13	Proposer's understanding of the scope of security tasks under the project, responsibilities and processes for monitoring adherence to those requirements, and security controls and their applicability in the solution.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Clearly describe expected scope of cybersecurity-related tasks under this contract and who (e.g., contractor, government) is responsible for executing those tasks.			
	Also clearly describe how you will monitor service and development processes to ensure adherence to the security requirements of this contract.			
	In providing these descriptions, clearly articulate the security controls you intend to employ in the solution. Include hardware, software, and physical security measures, the risks that they mitigate, and any residual risks resulting after implementation of these controls.			
Good Responses	Provides clear explanations of how the proposer will manage cybersecurity risk throughout and beyond the period of performance.			
	Provides a specific standard or known set of controls. Descriptions include which controls apply to the specific work and why some controls do not apply. These descriptions should demonstrate knowledge of the standard and how it applies to the work at hand.			
Bad Responses	Generic statements of implementing security measures throughout all aspects of the project.			
	Vague statements that implementations will follow standards, even a specific standard, but no demonstration of experience implementing the standard or standards.			
Tips	The extent to which a proposal can define the expectations and responsibilities can provide insight into the preparedness of the proposer to address cybersecurity challenges. At a minimum this must include access controls, storage location(s) for data at rest, authorization to storage location(s), implementation of secure transport (confidentiality and integrity), and logging.			
	The proposer should be able to show how controls align with your desired best practices. To that end, it's reasonable to request that the proposal include a mapping to best practices documents such as the CIS publication, the Essential Guide to Election Security.			
References and Links	CIS's Essential Guide to Election Security[11]			

[11] https://essentialguide.docs.cisecurity.org/en/latest/README.html

Table 14: Best Practice #14: Threat Environment Analysis

Number	Name	Category	Applicability	IT type
14	Proposer's understanding and staying aware of the threat environment, its proposed risk mitigation approaches, and identification of any residual risks.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide a description of the threat environment as it applies to the systems and their interconnections that are addressed in your proposal. Provide an assessment of the severity of threats, and identify and align mitigation approaches to the threats. Also, provide an assessment of the residual risks following mitigation actions.			
	Describe how you monitor ongoing security threat changes and respond to evolving threats, including monitoring common vulnerabilities and exposures (CVEs) and any ability to receive and share real-time threat information. Indicate participation in information sharing networks, including the Information Technology Information Sharing & Analysis Center (IT-ISAC), the Multi-State ISAC (MS-ISAC), and others.			
Good Responses	Actual risks are shown, usually in a table that lists, for each threat, the risk likelihood and consequence presented by the threat—usually in low, medium, and high—both pre- and post-mitigation. Mitigation approaches are listed for each threat to show how likelihood and consequence changes. Mitigated risks are realistic; it is unrealistic for all risks to be mitigated completely.			
	Proposer should participate in information sharing networks such as the MS-ISAC or other similar organizations. If not a member of the MS-ISAC, the proposer should commit to being sponsored for membership if awarded a contract.			
Bad Responses	Proposer claims there are no risks or that they can be completely mitigated in all circumstances. No acknowledgment of residual risks. No stratification (e.g., low, medium, high) of initial or residual risks.			
	Failure to identify concrete sources of cyber threat information.			
Tips	This should be a listing of expected threats to your systems and how those threats will be mitigated by the proposer. This listing should be thorough and indicate significant thought.			
	If the proposer has had a risk assessment performed internally or by a third party, ask to see their latest risk assessment.			
	The decision of the acceptable level of residual risk is yours. The proposer should be providing you a realistic evaluation of residual risk, acknowledging that no solution is perfect.			
	Not knowing or understanding ISACs is not disqualifying, but the proposer should be open to leveraging additional sources of security and threat information.			
References and Links	CIS's MS-ISAC[12]			
	IT-ISAC[13]			

[12] https://www.cisecurity.org/ms-isac

[13] https://www.it-isac.org

Table 15: Best Practice #15: Data Transmission

Number	Name	Category	Applicability	IT type
15	Processes for moving information, whether digitally or physically, to ensure that security is maintained at all times. This includes moving vote data, such as for tabulation or election night reporting. Specific focus on security requirements that apply to information and communication products or services.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Describe your process for moving data, whether digitally or physically, while maintaining appropriate security protection and data integrity. This includes between organizations such as the proposer and proposed subcontractors, and to the government, where applicable, during transitions to new systems and technologies.			
	Also, specifically describe security requirements that apply to information and communication products and services.			
Good Responses	For digital transfer of data, describes both data-in-motion requirements for secure communications (e.g., transport layer security (TLS), hypertext transfer protocol-secure (HTTPS)) and authentication requirements.			
	For physical movement of data, describes physical security approaches, including tamper-evident seals as well as chain-of-custody monitoring.			
	For deployment of new systems, describes expected downtime, backup procedures, and data security approaches during the transition.			
Bad Responses	Describes only that secure approaches are taken without describing specific measures for establishing secure transport of information.			
Tips	These days, it's standard to use HTTPS for secure communications everywhere.			
	There may be two separate policies or processes: one for the solution and one for transferring data between you and company. They should only differ in that the policies and processes for communication amongst one another may solely be documented process, whereas the policies and processes for HW and SW you are purchasing should be baked in.			
	The proposed approach should align with a commitment to patching systems to ensure the latest security protections are in place, such as implementing the highest level of encryption standards.			

Table 16: Best Practice #16: Controls Implmentation

Number	Name	Category	Applicability	IT type
16	Proposer's agreement to implement a specific set of security controls such as the CIS Critical Security Controls	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Describe the specific security controls that you will implement. These may be international information security standards such as ISO 27000 or common sets of controls specific to elections, such as those described in the Essential Guide to Election Security.			
Good Responses	If the government provides a set of controls, confirmation that the proposer will implement them. If the government does not provide a set of controls, the contractor should specify controls or principles it considers best practice.			
Bad Responses	If provided: failure to confirm that the proposer will adhere to the set of controls.			
	If not provided: failure to identify a candidate set of controls or best practices that the contractor believes will appropriately mitigate risk.			
Tips	Include any set of security controls to which the proposer should adhere. Ideally this will be a public, recognized set of controls, but controls specific to your organization are OK too, whether as the primary set or in addition to others.			
References and Links	CIS's Essential Guide to Election Security[14]			
	ISO 27000 family[15]			
	NIST Special Publication (SP) 800-53[16]			

[14] https://essentialguide.docs.cisecurity.org/en/latest/README.html

[15] https://www.iso.org/isoiec-27001-information-security.html

[16] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Table 17: Best Practice #17: Acceptance of Security Practices

Number	Name	Category	Applicability	IT type
17	Proposer's willingness to adhere to your organization's established security practices.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Confirm that you will adhere to the required security practices under this contract. *[Note: Be sure to provide reference to the security practices or a link to them.]*			
Good Responses	Confirmation that products and services will adhere to the required security practices. Describes experience implementing the same or similar security practices. References copy of proposer's own information security plan or practices.			
Bad Responses	No demonstrated experience implementing similar security practices or a lack of clear commitment to properly implement them as a part of this contract.			
Tips	Proposer should be willing to provide a legal attestation to remain compliant with the jurisdiction's cyber and information security policies, standards, and guidelines.			
	Proposer should affirm that any changes in requirements will be accomplished within a reasonable, specified time frame.			
	Ask for the proposer's own information security plan to show alignment with your organization's established security practices.			

Table 18: Best Practice #18: Security Service Level Agreements

Number	Name	Category	Applicability	IT type
18	Service level agreements (SLAs) for security that can be defined and agreed to as a part of the contract that address day-to-day activities and activities around an election.	Process	All systems	Hardware, Software, Services, Cloud
Suggested Language	Define specific levels of service for key work activities including performance standards for each service.			
	Expected outcomes for normal security activities and, separately, around the time of elections.			
	Include your policies for response time, types of support (e.g., in-person, phone) provided, and approach to ensuring continuity of mission critical services (e.g., failure restoral, patching and updates, and other relevant service component failures).			
	Clearly describe trigger points for deploying updates and the approvals needed on both the vendor and government sides. This response should address vulnerability detection and remediation, patching speeds, and incident response and escalation procedures.			
	For those products that cannot be readily updated, describe controls and monitoring that will be used to identify suspicious access or activity.			
Good Responses	Clear descriptions of pre-established measures of success that define specific quantitative goals that are stratified and provide definitions for each level (e.g., response of 15 minutes for critical issues, two hours for major issues). Specifies remediation actions for failure to achieve stated goals. Patching schedules and triggers for out-of-cycle patching are defined. Approval requirements are clearly defined. Clearly demonstrates sufficient capacity to be able to deliver according to the agreement. Demonstrated understanding of changing needs around an election.			
Bad Responses	Not clearly defined service levels and normal maintenance/support functions. Solely an as-needed patching schedule with no definition for “needed.” No description of which approvals are necessary to approve deployment. Lacks specifics for goals or provides qualifiers to statements such as “usually” or “typically.”			
Tips	Patching is a vital part of all hardware and software. Well-defined policies for patching should describe how, when, and with what approvals patching will occur, including any institutional steps required, such as re-certifications with the EAC.			
	While the proposer should include an SLA in its RFP response, details of that SLA are commonly negotiated.			
	SLAs should address patch and update management procedures for all systems managed by the proposer. Changes should generally be made on pre-production systems for testing prior to changes to production systems. The proposer should outline the request, approval, and testing process for emergency changes (i.e., critical changes with a limited window to apply to production).			

Table 19: Best Practice #19: Lifecycle Management

Number	Name	Category	Applicability	IT type
19	Proposer's experience in using standardized information technology lifecycle management processes for the exact scope of work. Includes proposer's lifecycle approach for development of its own hardware and software.	Process	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Do you have a standardized lifecycle management process for information technology?			
	If so, describe your experience in using that lifecycle management process for work of the same scope as this project. Describe the lifecycle processes used to manage hardware and software. How will these processes ensure that updates appropriately address security considerations?			
Good Responses	Describes defined, repeatable processes and adherence to standards and standard processes such as ITIL or Control Objectives for Information and Related Technology (COBIT). Provides concrete examples of prior use of the process in its work.			
	The proposer should use modern tools that are augmented by human inspection to validate that changes to do not degrade security.			
Bad Responses	Failure to describe a previously defined and demonstrated lifecycle process used in management.			
Tips	You may want to tailor this question to meet the type of procurement you are conducting. For instance, if data management is a primary aspect of this work, this would be a data lifecycle. If it is an IT hardware or software product, detailing the product lifecycle approach most appropriate, to include, for example, development, service and maintenance, and transition planning. For a service, a project management lifecycle would be most appropriate.			
	You may want to specify that the proposer periodically provide a comprehensive list of all assets, including serial numbers, hardware and software versions, when they were last serviced, patched, updated, and upgraded (i.e., a transaction log of service on each piece of equipment). The service logs should provide sufficient data for you and the proposer to know when it needs to be upgraded, updated, or replaced, based on the policies, procedures, and contractual arrangements.			
References and Links	Introduction to IT Infrastructure Library[17]			
	COBIT 2019[18]			

[17] https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html
[18] http://www.isaca.org/COBIT/Pages/default.aspx

Table 20: Best Practice #20: Security Plan

Number	Name	Category	Applicability	IT type
20	Security plan for proposed work.	Process	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Provide the security plan for implementing the security requirements and controls for the product or service. In the absence of the detailed plan, provide an outline of such plan along with examples of security plans for similar products or services provided under similar contracts you have been awarded and successfully implemented. The plan will be finalized in coordination with the government during the period of performance. If using a reference standard to develop your security plan, please identify which one.			
	As part of this, include whether you have a responsible disclosure policy for vulnerabilities and, if so, include it with your submission.			
	Describe the scope of responsibilities, assignment/ownership of tasks, and processes and procedures for adhering to security requirements and controls for the product or service.			
Good Responses	Implementation plans should define security tasks, responsibility for tasks, and criteria for assessing adequacy of task results. Proposers should be realistic and assign responsibility in a meaningful way with consequences. Especially in an operation like elections that has strictly defined deadlines, proper planning matters. It will describe risks to the timeline and approaches to mitigating those risks. It should demonstrate an understanding of potential barriers, such as applicable laws and regulations or formal approval processes.			
Bad Responses	Poorly developed implementation plans typically feature unrealistically aggressive timelines, oversubscribe resources, and underappreciate the potential for bumps along the road. An absence of or lack of detail in basic project management tools such as Gantt charts and hand-waving of risks are hallmarks of bad implementation plans.			
Tips	Implementation is the "who" and "how." A security implementation plan should describe the process of reaching a desired end state. In addition to basic timelines for implementation, it describes roles and responsibilities, resources needed to get the job done, and transition management.			
	Specifically request that risks be carefully addressed and provide some known risks (e.g., implementation is not complete by the freeze period prior to an election) and ask for their mitigations.			
	A system security plan (SSP) should be developed in accordance with a reference standard (like NIST SP 800-18) and should include information on how periodic auditing of the deployed system against the SSP will be performed to demonstrate continuing compliance. It should also address roles and responsibilities of contractor and government in achieving a formal Authorization to Operate, or ATO, if that is required in your jurisdiction.			
References and Links	NIST SP 800-18[19]			

[19] https://csrc.nist.gov/publications/detail/sp/800-18/rev-1/final

Table 21: Best Practice #21: Security Monitoring

Number	Name	Category	Applicability	IT type
21	Proposer's processes for monitoring adherence to standard information and physical security processes in its products and its own operations.	Process	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Describe your regular security audits and penetration analysis performed. Provide annual security audit reports conducted by an independent auditor.			
	Are you willing to be subjected to external analysis and penetration testing by an organization of our choosing? This may occur during planning , implementation, post-implementation, or operations.			
	Provide examples of prior security testing and evaluation reports, vulnerability assessment reports, and any related reports.			
	Additionally, the government may require contractors and their suppliers to provide security testing reports and independent audit reports from similar work to this project that details the effectiveness of security controls and demonstrates timely correction of issues.			
Good Responses	Contractor can provide history of past audits and penetration testing and resolution of findings. These should demonstrate sound processes and timely risk mitigation. They will show identified risks and mitigations. They should reflect adherence to a common standard or set of rules.			
	Permission to conduct reviews and testing at any time during the contract using the government's chosen auditors (e.g., state auditors, National Guard, the RABET-V® program, independent assessment specialists).			
Bad Responses	Summaries clearly written for this proposal or a generic statement of auditing practices. Submitted reports are incomplete or fictitious examples and do not contain recognition of risks that need mitigation.			
	Limits on reviews or insistence on the proposer conducting internal reviews.			
Tips	Vulnerability reports should cover not only assets deployed for your specific project but also for core contractor functions and services, such as vulnerabilities in those systems as well as your production/UAT/QA/test systems).			
	Claiming proprietary limitations is not acceptable, especially if a nondisclosure agreement is in place. The proposer may redact items to protect the identity of clients. Often, you will not get a full report, but rather a summary showing findings. There may also be restrictions on sharing this information publicly.			
	Products should be subject to review before acceptance. Any item altered through a service contract should similarly be subject to review. The contractor may wish to limit the frequency with which audits or testing occur. A reasonable frequency is once or twice annually or whenever a new product is deployed.			
	It is normal for vulnerability and penetration test results to have residual issues. The contractor explain false positives and address why any unaddressed high or critical priority issues. The contractor must be able to provide you procedural or other mitigations they have in place.			
References and Links	CIS's RABET-V Program[20]			

Table 22: Best Practice #22: Security Certifications

Number	Name	Category	Applicability	IT type
22	Companywide process certifications and demonstrated adherence to proposer's documented processes.	Process	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Provide evidence of certification or registration according to national quality or security standards. Describe your adherence to standardized quality principles, such as through registration as ISO 9001 (general quality) and ISO/IEC 27001 (information security). Both are strongly preferred. If you do not follow a standardized quality principle, provide your documented processes and evidence that you monitor adherence to those processes.			
Good Responses	Up-to-date proof of certified adherence to both standards. Organizations should be able to submit verifiable proof. Proposer can provide evidence of past testing and evaluation and related reports.			
Bad Responses	Claims of adherence without certification. Claims of following an alternate approach that is not a well-recognized standard. Lack of evidence of testing and evaluation history.			
Tips	Standardized quality principles are an objective way for an organization to demonstrate that it understands and adheres to industry best practices. It may be acceptable for an organization to not adhere to these principles, but, if so, it should be able to explain its rationale for not doing so.			
	Smaller organizations are less likely to have these certifications. At a minimum, they should be able to provide evidence they have and follow documented processes.			
	Organizations will often state their certification but not provide documentation. If an organization claims certification to a standard, ask for proof.			
	If an organization says it adheres to a standard but is not certified, it should have evidence of its own internal evaluations. These are not just checklists, but detail how the organization manages its processes. There are some instances, like with EAC certification, in which you should consider requiring certification.			
References and Links	ISO 9001 Quality Management[21]			
	ISO 54001 Application of ISO 9001:2015 for electoral organizations[22]			
	ISO 27000 family[23]			

[20] https://www.cisecurity.org/elections/rabetv

[21] https://www.iso.org/iso-9001-quality-management.html

[22] https://www.iso.org/standard/75288.html

[23] https://www.iso.org/isoiec-27001-information-security.html

Table 23: Best Practice #23: Supply Chain Management

Number	Name	Category	Applicability	IT type
23	Proposer's supply chain management and selection process for suppliers, including contractor's approach to evaluating replacement components or new technologies evaluated for use in the environment to ensure adequate security.	Process	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Detail your approach to supply chain management, including the selection process for suppliers. Provide specific information including, but not limited to:			
	How is information regarding supply chain issues shared among the organization and suppliers? How do you handle content originating from non-U.S. sources?			
	How do you review suppliers and their products to ensure that they do not contain security vulnerabilities or malicious content and are free from unexpected or unwanted procedures?			
	Which processes are used to monitor compliance of suppliers to requirements of the contract? Describe any process for auditing suppliers' ability to maintain security in their development process.			
	What is your process for managing hardware and software that is no longer supported by the supplier to ensure continued maintenance of appropriate security? Describe your transition process for changes in suppliers to ensure security measures are continually met. How will you maintain appropriate communication with the government for such products?			
Good Responses	Processes described provide confidence that proposer carefully evaluates origins and specific security characteristics of new technology or replacement components. The response should describe compliance monitoring requirements, testing practices, work locations, certifications, and supply chain risk management activities, such as requiring suppliers to follow established best practices such as NIST SP 800-161.			
	Recognition of limitations in the updates process, such as that older components may not receive updates and that updates may be complicated by certification procedures. For those products that can be readily updated, description of a clear process for making updates and notifying the government when updates are available and the approach to implementing the update.			
Bad Responses	Statements that the contractor uses only genuine or quality components without any reference to a process, quality assurance, or requiring suppliers to implement specific controls.			
Tips	It may be appropriate to rely on an outside evaluator to assess new technology and replacement components.			
	Open source software can be OK to use as part of a solution, but it should be long-standing, well-vetted software. Open source software can be as or more secure than proprietary solutions, but it, like all software, must mature.			
References and Links	NIST SP 800-161 Supply Chain Risk Management[24]			
	CISA Resources for Supply Chain Management[25]			
	CIS's Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers[26]			

Table 24: Best Practice #24: Accessing Sensitive Information

Number	Name	Category	Applicability	IT type
24	Processes for managing and documenting access to different categories of sensitive information.	Process	Operational Systems	Software, Services, Cloud
Suggested Language	Describe how information sensitivity is categorized and how access to sensitive information is managed and documented for each category, including your ability to create reports and machine-readable data extracts for both private and public dissemination. Clearly designate responsibilities, obligations, and procedures for key aspects of a data governance plan (data owner, data steward, data retention, information sensitivity, etc.). Demonstrate your understanding of this jurisdiction's data governance policies and practices and propose a data governance approach as part of your submission.			
	Your response should include how various categories are treated when transmitted, such as when and how information is digitally signed and encrypted.			
Good Responses	Acknowledges and properly addresses that different types of data have different sensitivities. Provides a sufficient stratification to address the different needs and describes appropriate controls for each. Should include descriptions of the types of data anticipated in the product or throughout the course of the project (e.g., voter personal information, candidate filings, precinct records).			
	Proposer provides a clear data classification scheme and also describes how it will be continuously applied to data in the system(s).			
Bad Responses	Describes an approach in which data are secured "as needed" or with "appropriate" security without clear thought on the types of data that will be encountered under the proposed work.			
Tips	Proposer should affirm their acknowledgment and acceptance of requirements for jurisdictions to easily comply with a jurisdiction's laws around providing non-sensitive public reports and data subject to your open records/open data laws within the timeline required under those laws.			
	At minimum, the plan should describe which categories are signed and which are encrypted. For example, you should expect to see transmitted data of importance signed, while sensitive data should be both signed and encrypted.			

[24] https://csrc.nist.gov/publications/detail/sp/800-161/r1/final

[25] https://www.cisa.gov/information-and-communications-technology-supply-chain-risk-management

[26] https://www.cisecurity.org/about-us/media/press-release/center-for-internet-security-cis-releases-new-elections-technology-cyberse

Table 25: Best Practice #25: Controls on Data Access

Number	Name	Category	Applicability	IT type
25	Controls on data and access, including where the data reside, who has access, and how access rights are maintained; encryption approach; and incident capabilities, including logging and forensics.	Technology	All systems	Hardware, Software, Services, Cloud
Suggested Language	Describe in detail the controls placed on data and access to data. Include requirements for location, access rights, maintenance and enforcement of access rights, encryption, incident response and backup capabilities, and logging and forensics capabilities.			
Good Responses	All controls should have clearly documented policies. For each control, the contractor should either include a link to the policy or describe the recommended control or control options. Though most applicable to cloud service providers, this also applies to first-party providers in which the contractor provides data management or the government manages controls. In the latter case, it should detail the options for managing controls available to the government and the manner in which those controls are managed.			
Bad Responses	Overly optimistic statements that the provider can implement any required controls.			
Tips	Logging of events should follow a common data format, such as NIST SP 1500-100.			
	Look for data handling to include encryption for data both while in transit and while stored at rest.			
	Access to the data is restricted to only those with the need to see it, by established and documented access control methods.			
References and Links	NIST SP 1500-100 Election Results Common Data Format[27]			

[27] https://www.nist.gov/itl/voting/interoperability/election-results-reporting-cdf

Table 26: Best Practice #26: Cloud Security

Number	Name	Category	Applicability	IT type
26	Cloud security options.	Technology	All systems	Cloud
Suggested Language	If the solution will be hosted in a cloud or multi-tenant environment provided by Azure, AWS, or Google, include information on the adherence to the appropriate CIS Benchmark for Cloud Service Offerings. Explain the reason for any deviation from that Benchmark and provide any additional options that are available.			
	If using another cloud provider, include the full menu of security options and services offered by the hosting provider, and which specific security options and services are included in the proposal.			
Good Responses	The proposer should include all security options that are available, whether or not they will be used. While it's not necessary to justify every decision, the chosen set should make sense.			
Bad Responses	Anything less than the full list of security options.			
Tips	The goal of including the full menu is to see what the provider has available. You may want to include a different set of security options as part of negotiations.			
	Look for implementation of the solution in an approved "Gov" cloud with FedRAMP baselines of high and moderate, or the equivalent. This would cover many of the key security components, but documentation should be provided showing that secure features are enabled, such as encryption at rest.			
	Be sure to ask about specific data compliance requirements in your state and jurisdiction. For instance, many states require cloud providers to keep all data within the United States. If you have this requirement, be sure to explicitly ask about it.			
References and Links	CIS Benchmarks[28]			
	FedRAMP Cloud Service Providers[29]			
	FedRAMP Marketplace[30]			

[28] https://www.cisecurity.org/cis-benchmarks/

[29] https://www.fedramp.gov/cloud-service-providers/

[30] https://marketplace.fedramp.gov/

Table 27: Best Practice #27: Open Standards

Number	Name	Category	Applicability	IT type
27	Use of open standards and common approaches in software and common data formats.	Technology	All systems	Hardware, Software, Services, Cloud
Suggested Language	For user- and client-specific software and applications, confirm on which types of systems and, where applicable, browsers the product will have full functionality. In general, products should be fully functional on a host of systems, to include netbooks (such as Chromebooks) and all major browsers.			
	If managing voter or ballot data, provide the data format(s) you are using and identify common functions supported with those formats (e.g., risk-limiting audits).			
Good Responses	Applicable products are fully functional across a host of systems and browsers or, if not, a full description is provided as to why this is not possible.			
Bad Responses	A lack of planning or formalized decision around the approach. Support only for specific browsers or systems that don't represent the whole of your environment.			
Tips	Development toward specific systems—even if they are the only systems you have in your environment—is generally frowned upon. This goes beyond compatibility: if something is developed in such a way that it only functions on a specific system, this may indicate that the proposer is not using the most common, and thus best-vetted, standards.			
	While it is good to have flexibility to work across multiple versions of a browser, it should be expected that the software will be maintained to use the most current or very recent versions and have a policy of deprecating older versions that are no longer secure.			
	Security audit functions are typically performed outside of the system and thus it is important that systems make data available for auditing in common formats that meet the auditing needs of the election officials.			
References and Links	NIST SP 1500-100 Election Results Common Data Format[31]			

[31] https://www.nist.gov/itl/voting/interoperability/election-results-reporting-cdf

Table 28: Best Practice #28: Security Architecture

Number	Name	Category	Applicability	IT type
28	Security architecture for proposed or required solution.	Technology	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Provide a full description of the proposed solution’s security architecture. Describes completely how architecture will ensure security of election infrastructure.			
Good Responses	A good response will provide diagrams, examples of mitigation of threats and risks, and descriptions of a proposed security architecture. It should demonstrate that the proposer understands their systems and how they fit into the larger context. It should include descriptions of all system components and detail multiple layers of security, internet connections, firewalls, intrusion detection and prevention systems, and other critical components. It should describe the security approach for each aspect of the system.			
	When drafting a proposal, it’s often difficult to determine how much detail to provide, especially if there are page limits. Concisely written proposals are a signal that a vendor has put thought into their work. For this reason, it’s important to make it clear that the successful proposal will provide significant details on their approach to security.			
Bad Responses	It’s OK for vendors to make claims that they use security approaches that are “state of the art,” “best in class,” “military grade,” or the like, but they need to back up those claims with details of security architectures and processes.			
Tips	Most proposers will be reluctant to provide detailed information in a public document (assuming your jurisdiction’s laws require bid materials to be public). Work with your procurement team to allow for confidentiality of detailed security architecture information in your solicitation.			
	Expect layered architecture that partitions most sensitive data/critical systems from less critical/sensitive ones.			
	It’s OK to put a page limit on proposals, but allow for additional pages for diagrams of security approaches. If a vendor has implemented in a similar environment, they’ll be able to provide detailed diagrams fairly easily. This can help officials identify the best qualified proposers.			
	Some (or most) of your solicitation reviewers may not have the breadth or depth of technical knowledge to assess detailed security architecture materials. Consider carving out an assessment of these materials to a separate group of tech reviewers and incorporate their findings/ratings into the other evaluation materials.			

Table 29: Best Practice #29: Cryptography and Key Management

Number	Name	Category	Applicability	IT type
29	Approach to cryptography and key management for data security	Technology	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Describe your approach to cryptography, including which cryptographic modules and protocols you use, and how you conduct key management and manage the secrecy of private keys, if applicable.			
Good Responses	Demonstrates understanding of where cryptography can and should be employed as well as familiarity with different types of cryptography and the rationale for the selection of the specific cryptographic solution proposed. In addition, thoroughly addresses cryptographic key management including protection of keys.			
Bad Responses	General descriptions of the use of encryption as a means to protect data at rest or in transit.			
Tips	Use of standard cryptographic modules is a must. We highly encourage you to permit only cryptographic modules validated under Federal Information Processing Standard (FIPS) 140-2.			
	This best practice is intended for specialized applications leveraging cryptography. Standard encryption, like websites with HTTPS, should be on all systems.			
References and Links	FIPS 140-3 Requirements for Cryptographic Modules[32]			
	FIPS 140 Validated Modules list[33]			

[32] https://csrc.nist.gov/publications/detail/fips/140/3/final

[33] https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

Table 30: Best Practice #30: Software and Asset Ownership

Number	Name	Category	Applicability	IT type
30	Ownership of software and other assets.	Technology	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	If the proposal includes commercial off-the-shelf (COTS) or modified off-the-shelf (MOTS) software, address ownership of the software and design assets both during the project and afterward. Also, address whether source code and other artifacts will be held in escrow or delivered to the government during the project, and ownership of IP rights at the end of the project.			
Good Responses	Addresses ownership of all assets in the project, including software licenses and software developed (or modified) as part of the project.			
	Includes statements that code will be delivered to the government, put in software escrow, or a similar mechanism to ensure that the government won't be left with a build that can't be updated should the proposer go bankrupt or otherwise cease operations.			
Bad Responses	Insufficiently addresses ownership. The government should own licenses for COTS and MOTS software and should have a process for accessing source code for any proposer that has even a small risk of going out of business.			
Tips	Some companies may not be willing to participate in software escrow. This may be OK, especially for larger, more established companies (such as Microsoft®) that are unlikely to go bankrupt and over which you have little contracting leverage. But for smaller organizations, the risk of failure is higher and should be mitigated.			

Table 31: Best Practice #31: Solution Certifications

Number	Name	Category	Applicability	IT type
31	Certifications received for the solution, including EAC, RABET-V verification, and applicable state or local security standards. Or, in lieu of certification, rationale for lacking certification and approach to ensure that security in the solution is mature and reliable.	Technology	Operational Systems	Hardware, Software, Services, Cloud
Suggested Language	Detail certifications obtained for the solution(s) you intend to deploy and how these meet applicable federal, state, or local security standards. If the solution(s) will not be certified, how will you ensure mature and reliable security? Additionally, describe your process for ensuring the certified system will be updated to reflect current security patches and updates to underlying components (e.g., operating systems, databases, communications systems).			
Good Responses	For products with a known certification process, evidence of certification. For other products, a clear process for assessing security. For all products, a clear description of how updates will occur and how that affects certification or other validation processes.			
Bad Responses	Lack of demonstrated knowledge of certification processes. Lack of procedures or assessing the security of implementations.			
Tips	You will likely want to modify this question for the given Type of procurement, Especially when thinking of voting systems vs. non-voting election systems vs. backend COTS IT systems.			

Table 32: Best Practice #32: Protection of Personal Information

Number	Name	Category	Applicability	IT type
32	Personal information management, including transmission and approach to protection.	Technology	All systems	Software, Services, Cloud
Suggested Language	If personal information will be handled, describe how you will manage the minimization, collection, storage, and transmission of that personal information. Describe confidentiality and privacy approaches with regard to personal information.			
Good Responses	Gives attention to minimization of personal information as a first measure for reducing risk.			
	Where personal information must be collected, gives a thorough response for managing personal information through data security at rest and in transit. Provides anticipated encryption techniques and secure communication protocols.			
Bad Responses	Suggests only that personal information will be protected at all times, without describing specific approaches.			

Table 33: Best Practice #33: Endpoint Protection

Number	Name	Category	Applicability	IT type
33	Advanced endpoint protection on core systems.	Technology	All systems	Hardware, Software, Cloud
Suggested Language	Confirm that you have advanced endpoint protection for any server or workstation that is part of the core service offering. All systems accessing the core service offering must have advanced malware detection along with traditional anti-malware software. Specifically, the advanced malware software must allow root-cause analysis with forensics showing how infection occurred along with actions malware took.			
Good Responses	Explicit confirmation that the relevant systems meet the requirements for advanced endpoint protection. The proposer should be able to provide details on how it employs this endpoint protection.			
Bad Responses	General statements of endpoint protection without a description of the specific software used or its capabilities.			

Table 34: Best Practice #34: Specific System Experience

Number	Name	Category	Applicability	IT type
34	Experience with the needed system or service.	Technology	All systems	Hardware, Software, Services, Cloud
Suggested Language	Provide details on relevant experience with the [specific system or service]. Details should include experience meeting the specific requirements, transitionin from past systems, and planning for future transition or end of life.			
Good Responses	Clear details that the proposer has installed, operated, or supported the relevant system or service and understands how to transition to and from it.			
Bad Responses	General statements of understanding the technology or unsubstantiated claims of being able to manage transitions.			

Table 35: Best Practice #35: Use of AI

Number	Name	Category	Applicability	IT type
35	Use of Artificial Intelligence in Products.	Technology	All systems	Hardware, Software, Services, Cloud
Suggested Language	Please describe any artificial intelligence (AI) or machine learning (ML) capabilities integrated into your solution. Include details on:			
	1. Specific AI/ML functionalities, their purposes, and ongoing maintenance and improvement.			
	2. Data sources used to train the AI/ML models.			
	3. Measures taken to ensure AI/ML fairness and mitigate bias.			
	4. Transparency and explainability of AI/ML decision-making processes.			
Good Responses	Provides specific functionality provided by AI/ML, including the modules impacted and whether its use is optional.			
	Provides quantative data, results of testing, and case studies with feedback.			
	Provides information on how models are trained, and that data represents a wide swath of related clients or activities to yours.			
	Details on auditing procedures for accuracy and bias including details of auditing your specific deployment for accuracy and bias as part of the onboarding process.			
Bad Responses	Focus on buzzwords, embellishments, or unfounded claims.			
	No demonstration of rigor around testing, research, and structured improvement to models.			
	Lack of details around training, training, datasets, and customization.			
Tips	Not all AI/ML is the same. Be sure to understand what types of AI are being used, particularly natural language processing and generative AI. Remember that, for instance, red-eye reduction on your phone is a form of AI, but isn't what we talking about here.			
	Even if doing everything "right," you may determine the risk is too great, depending on the sensitivity of the activity. If they can't make use optional and you feel there is a risk, don't use it.			
	Think about what data are being "touched" by the AI. Analysis of data is different from manipulation of data is different from interaction with voters, such as through a chatbot.			
	Thoroughly demo the AI features, including trial use.			
	Inquire about the vendor's AI ethics policy and compliance with relevant AI regulations.			
References and Links	Austrailian Cyber Security Centre's Engaging with Artificial Intelligence[34]			
	U.S. Office of Personnel Management's Responsible Use of Generative Artificial Intelligence for the Federal Workforce[35]			

[34] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/

artificial-intelligence/engaging-with-artificial-intelligence

[35] https://www.opm.gov/data/resources/ai-guidance/

CHAPTER FOUR

MODEL LANGUAGE

Hey there! We're working on this section and could use your help. If you know a procurement, or part of a procurement, that you really like, send it our way!

It can be an RFI, RFP, contract terms, or anything else you think would be helpful to share with others. Send any links or documents to elections@cisecurity.org and we'll include them in this section.

CHAPTER

FIVE

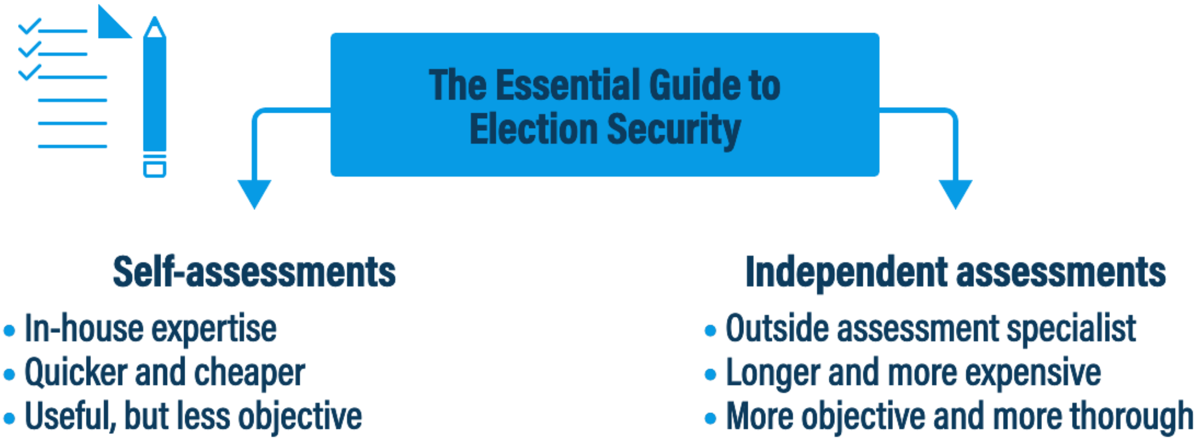
SECURITY RISK IN ELECTION TECHNOLOGY PROCUREMENT

5.1 Assessing Risk

All IT has risks. Efforts to mitigate some risks inevitably leave other risks unaddressed. Leaders must determine which risks are acceptable in the face of limited resources. To understand and prioritize their risks, all organizations should conduct regular risk assessments. Risk assessments can be sorted into two categories:

1. **Self-assessments**: In-house risk assessments are generally faster and less expensive while still providing useful insight into your cybersecurity posture. Good self-assessment options include the National Cybersecurity Review[36] (NCSR) and the CIS Controls Self Assessment Tool[37] (CSAT). MI-ISAC members can also use tools through CIS's SecureSuite[38], which is free to all members. You can also use the Essential Guide to Election Security[39] to help determine the appropriate best practices against which to assess your organization.

2. **Independent assessments**: Because they are conducted by outside assessment specialists, independent assessments usually cost more and take longer, but they are more objective and thorough. Where time and resources permit, they are preferable even when an organization has deep cybersecurity experience.



The Essential Guide to Election Security

Self-assessments

- In-house expertise
- Quicker and cheaper
- Useful, but less objective

Independent assessments

- Outside assessment specialist
- Longer and more expensive
- More objective and more thorough

[36] https://www.cisecurity.org/ms-isac/services/ncsr
[37] https://www.cisecurity.org/insights/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls
[38] https://www.cisecurity.org/cis-securesuite
[39] https://essentialguide.docs.cisecurity.org/en/latest/README.html

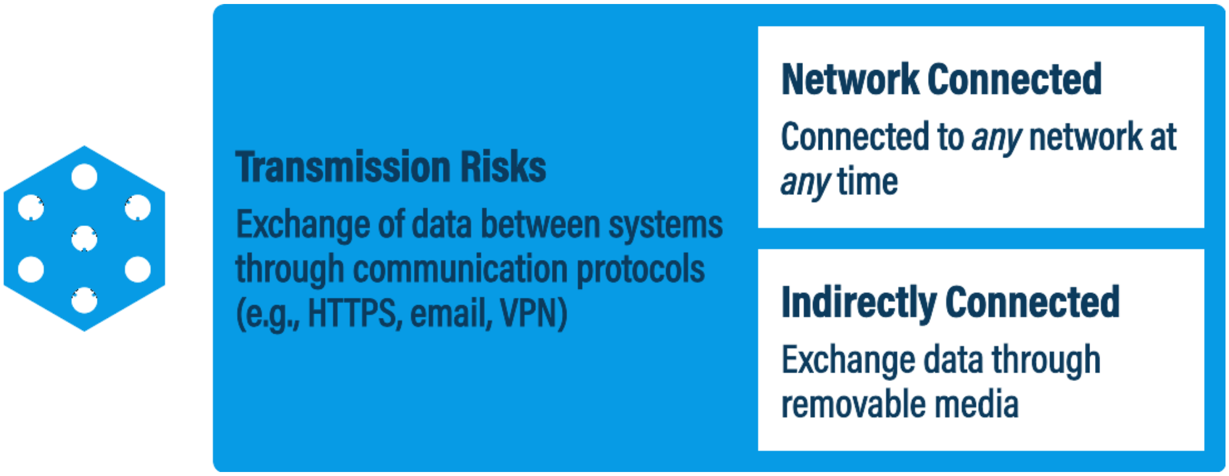
5.2 Organizational Risk

Risks in election infrastructure vary, but one defining characteristic is the type of connections it has with a networks or the internet. CIS has identified that the highest level of risk stems from those systems that are network-connected. That is, they are connected to any network (not just the internet) at any time. This network-connected category of risk includes most voter registration and election night reporting systems, and may also include ePollbooks, and, other non-voting election technology.

Systems not connected to a network still require careful assessment and prioritized mitigation of risks. These indirectly connected systems are never connected to a network. The exchange of data between them, and with other systems, occurs indirectly through removable media such as USB drives. Voting machines and tabulators typically fall in this category.

Beyond network-connected and indirectly connected systems and devices, an additional area of risk involves the transmission of data between systems. For example, ballot definitions and PDFs may be well-protected in the jurisdiction's systems but have risk introduced when they are emailed to a third-party to be physically printed.

These risks can and should be managed, and part of that process is understanding and managing cybersecurity risk in IT procurement.



Transmission Risks

Exchange of data between systems through communication protocols (e.g., HTTPS, email, VPN)

Network Connected

Connected to *any* network at *any* time

Indirectly Connected

Exchange data through removable media

5.3 Individual System Risk

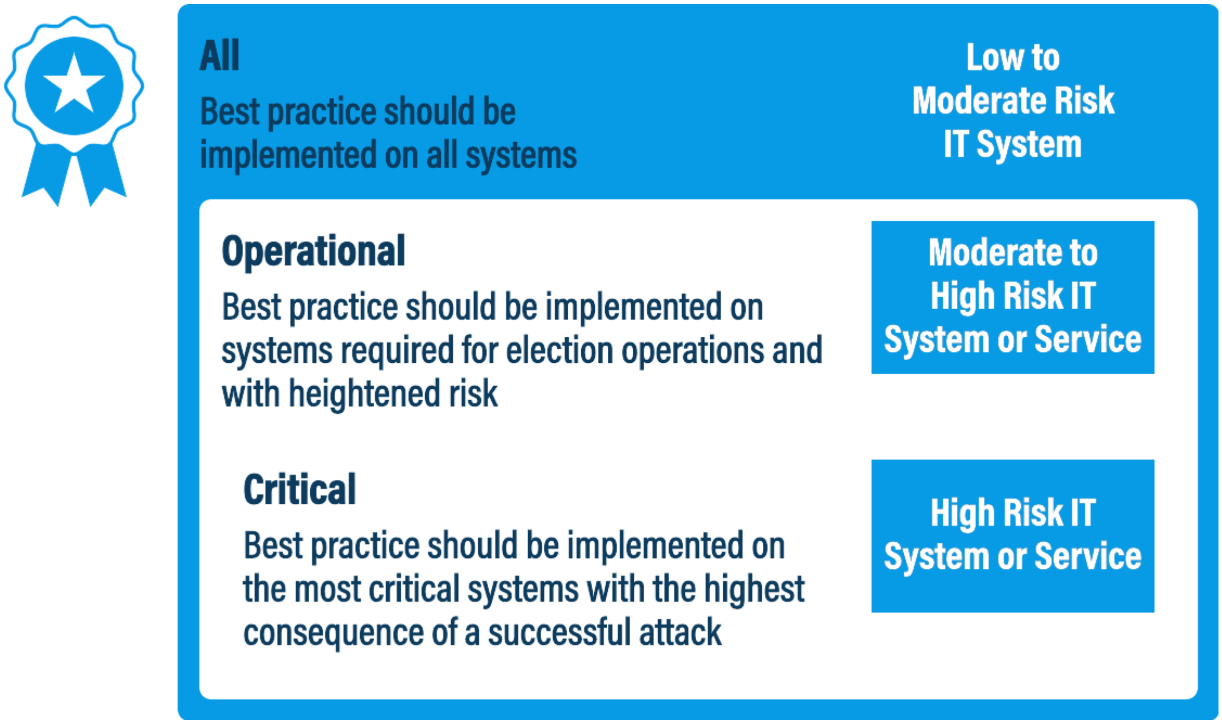
Most security controls impose a cost of some kind, whether time, money, reduced access or usability, or all of the above. Mandating that a vendor implement all possible security controls is often impractical or will undermine business objectives. This makes it critical to determine the right set of controls for any given system.

For that reason, we don't recommend applying all of the best practices in this guide to every system. Rather, some best practices should be implemented on all systems, others only on operational systems, and some only on critical systems. For instance, some basic website security measures should be applied to any system (so long as it has a website), while there are some advanced malware detection approaches that are expensive and difficult to implement and thus we recommend them for only critical systems.

One way to think about the application of these best practices is by considering whether a system is critical or operation. Operational systems should have more rigorous protections, while critical systems should have even the most stringent protections applied, so long as they are applicable to the system. The best practices have recommendations according to these three categories:

1. **All systems**: The best practice is a reasonable investment to expect for any type of election system. It is vital to ensure mitigation of the most common threats.
2. **Operational systems**: The best practice is a reasonable investment for systems that are important to successful election operations and thus carry greater risk. Systems with other security mitigations, backups, etc., may not need this best practice. Procurements of all critical systems and those with relatively high risks should implement the best practice.
3. **Critical systems**: The best practice is necessary only for critical systems, which is those with the highest consequence of a successful attack. These are typically the most expensive and difficult to implement best practices; requiring them will likely have an appreciable impact on the cost of your procurement but are likely necessary to reduce risk to an acceptable level.

These classifications serve as a starting point for differentiating between different types of systems in the elections technology procurement but should be tailored to meet the needs of a specific environment.



All
Best practice should be implemented on all systems

Low to Moderate Risk IT System

Operational
Best practice should be implemented on systems required for election operations and with heightened risk

Moderate to High Risk IT System or Service

Critical
Best practice should be implemented on the most critical systems with the highest consequence of a successful attack

High Risk IT System or Service

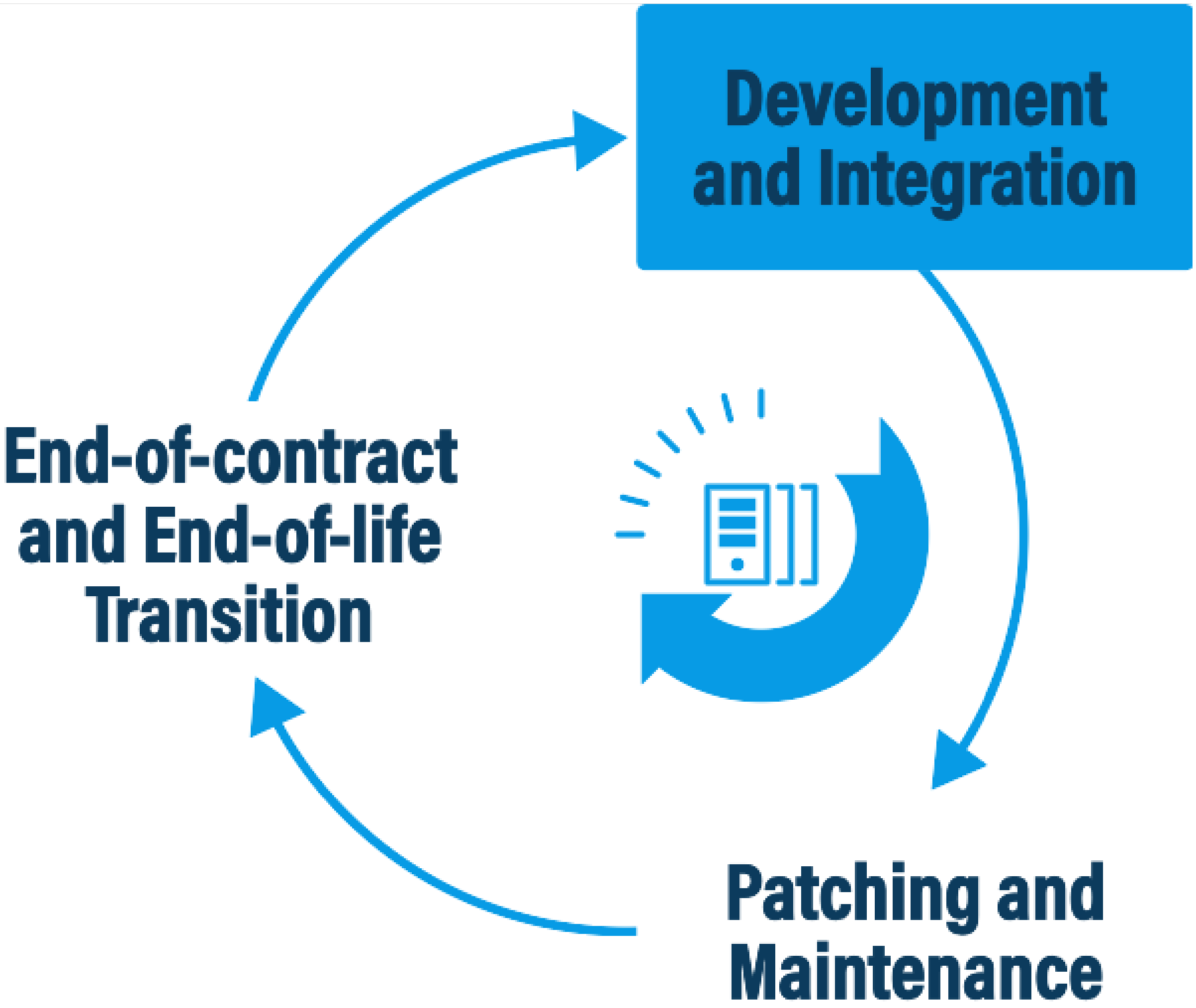
CHAPTER

SIX

THE IT LIFECYCLE

A very brief description of the IT lifecycle can help us understand the importance of different aspects of the procurement process. Descriptions vary, but generally the IT lifecycle can be described in three broad parts:

- **Development and integration**: Hardware and software must first be well designed. When a piece of hardware or software is poorly designed, there may be no way for the buying organization to meaningfully secure it. When designed well, it must then be properly implemented and integrated into the election infrastructure. This integration is sometimes part of the procurement of the hardware or software or could be managed by a separate operations team.
- **Patching and maintenance**: Even with a successful initial configuration and integration, organizations need to manage their IT in a continually changing environment. This requires up-to-date training for personnel, well-defined and executed security processes, and ongoing and effective management of services.
- **End-of-contract and end-of-life transition**: Organizations must understand the expected life of the hardware or software upfront and have a reasonable plan for replacing it. Vendors, especially service providers, should be prepared to work with election officials to plan for this from the beginning. This should also include transitions if a different vendor wins the contract.


Development and Integration
Patching and Maintenance
End-of-contract and End-of-life Transition

CHAPTER

SEVEN

SUMMARY OF BEST PRACTICES AND MODEL LANGUAGE

The following table contains a brief summary of all of the best practices in this guide. You can read the full best practices *here* (page 5).

Table 1: Summary of Best Practices

Number	Best Practice Name
1	Qualifications and experience of individuals proposed for work.
2	Demonstrated past performance performing proposed work. Includes awareness of, and experience adhering to, applicable certifications and legal and regulatory requirements.
3	Proposer personnel policies regarding hiring and conduct standards, including background check, citizenship, and visa requirements.
4	Proposer location(s) where work will be performed and equipment supported as well as administrative and facility security at the location(s).
5	Training procedures for the proposer.
6	Company ownership, board members, and stakeholders.
7	Proposer process for identifying and approving changes of key personnel who perform most critical management and technical functions.
8	Proposer authorization procedures for personnel with access to sensitive information and systems.
9	Proposer policies and practices for subcontractor personnel.
10	Proposer's regular process for identifying and remediating cyber risks, with particular focus on components and information that are critical for mission success and increased attention to these elements.
11	Security processes that include incident handling, recovery, and contingency arrangements to ensure availability. Includes incident response, such as when and how the government will be notified in the event of an incident.
12	Transition plan for the end of the contract.
13	Proposer's understanding of the scope of security tasks under the project, responsibilities and processes for monitoring adherence to those requirements, and security controls and their applicability in the solution.
14	Proposer's understanding and staying aware of the threat environment, its proposed risk mitigation approaches, and identification of any residual risks.

continues on next page

Table 1 – continued from previous page

Number	Best Practice Name
15	Processes for moving information, whether digitally or physically, to ensure that security is maintained at all times. This includes moving vote data, such as for tabulation or election night reporting. Specific focus on security requirements that apply to information and communication products or services.
16	Proposer's agreement to implement a specific set of security controls such as the CIS Critical Security Controls
17	Proposer's willingness to adhere to your organization's established security practices.
18	Service level agreements (SLAs) for security that can be defined and agreed to as a part of the contract that address day-to-day activities and activities around an election.
19	Proposer's experience in using standardized information technology lifecycle management processes for the exact scope of work. Includes proposer's lifecycle approach for development of its own hardware and software.
20	Security plan for proposed work.
21	Proposer's processes for monitoring adherence to standard information and physical security processes in its products and its own operations.
22	Companywide process certifications and demonstrated adherence to proposer's documented processes.
23	Proposer's supply chain management and selection process for suppliers, including contractor's approach to evaluating replacement components or new technologies evaluated for use in the environment to ensure adequate security.
24	Processes for managing and documenting access to different categories of sensitive information.
25	Controls on data and access, including where the data reside, who has access, and how access rights are maintained; encryption approach; and incident capabilities, including logging and forensics.
26	Cloud security options.
27	Use of open standards and common approaches in software and common data formats.
28	Security architecture for proposed or required solution.
29	Approach to cryptography and key management for data security
30	Ownership of software and other assets.
31	Certifications received for the solution, including EAC, RABET-V verification, and applicable state or local security standards. Or, in lieu of certification, rationale for lacking certification and approach to ensure that security in the solution is mature and reliable.
32	Personal information management, including transmission and approach to protection.
33	Advanced endpoint protection on core systems.
34	Experience with the needed system or service.
35	Use of Artificial Intelligence in Products.

CHAPTER

EIGHT

A PRIMER ON IT PROCUREMENT

Even for commodities, procuring IT is more than just buying a product or service—it's a process. The procurement process can be very complex and can vary widely from state to state and locality to locality. This guide does not address the specifics and particularities of any given jurisdiction; the goal of this appendix is to provide a basic description of procurement in general so that non-procurement staff and officials have a better understanding of the underlying process for executing a procurement.

8.1 The Procurement Team

It might be a stretch to say that it takes a village to execute a procurement, but there are a number of critical players involved:

- **Election officials**. From an internal perspective, election officials are the customer. Election officials should look to develop positive, collaborative relationships with other organizational functions, but should always remember that the top priority is their ability to achieve the outcomes they need. Election officials must maintain full understanding of what is occurring throughout the procurement process. As an election official, if something does not make sense, ask for clarification until you are satisfied. This is the role and right of the customer.
- **Procurement teams**. The role of procurement teams is to support election officials on the process and procedures of the procurement. They know how to properly execute contracts for goods and services within their jurisdiction. They are usually the final authority on whether a contract goes into force, but their overall role is to improve the manner in which programs and operational teams, such as election offices, execute their mission.
- **IT teams, including IT security teams**. Whether state or local, IT teams often help set guidelines for procurements and may also be involved in the evolution and execution of some procurements. IT teams may set requirements but may also play an advisory role. IT teams focus more broadly than security. Don't assume their perspective is to achieve the same level of security you want or that their input will result in better security outcomes. They are there to provide you support on the best practices for IT procurements, but as the customer you must use that information to assess the risks before making the final decision.

Election officials are the customer, and procurement and IT teams are there to help the election officials achieve their goals. While these different entities may be in the same organization, they may not always see the problem the same way. Together, by focusing on their respective roles, these teams can complete efficient and effective procurements.

8.2 Understanding Common Procurement Types

There are many ways to execute a procurement. Different procurement types are appropriate for different circumstances. This section will address three common approaches:

1. **Pre-negotiated contract**: This is an agreement established by a government buyer with a schedule contractor to fill repetitive needs for supplies or services (from GSA[40]). Pre-negotiated contracts include blanket purchase agreements (BPAs), indefinite quantity indefinite delivery (IDIQ) contracts, and schedule contracts, such as contracts awarded by the U.S. General Services Administration[41] and available for use by state and local government organizations.

2. **Lowest price technically acceptable**: The award is made for a specific organizational requirement on the basis of the lowest evaluated price of proposals meeting or exceeding the acceptability standards for non-cost factors (from acquisition.gov[42]).

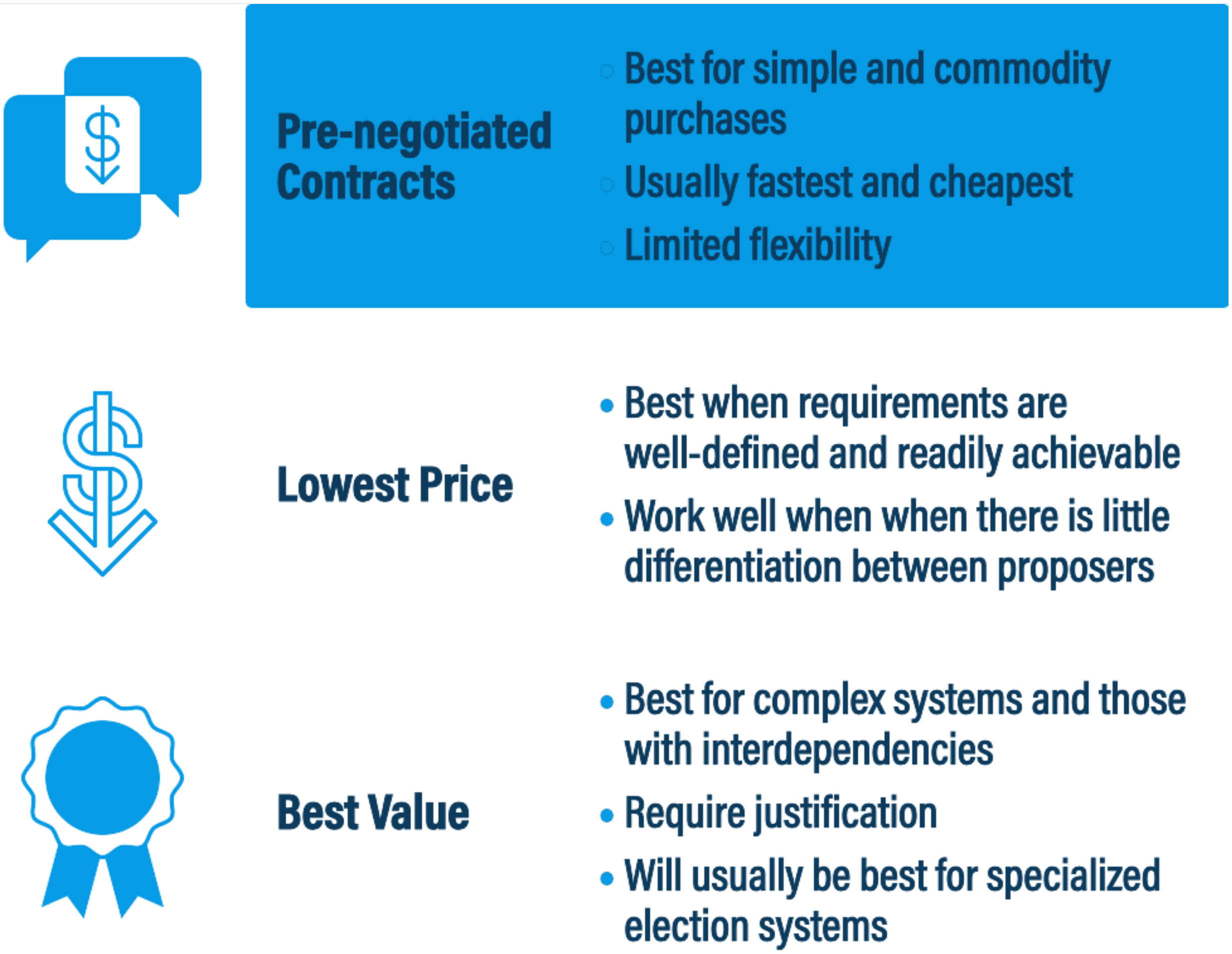
3. **Best value**: These refer to tradeoffs between cost factors and non-cost factors, and allow the government to award a contract for a specific organizational requirement other than the lowest priced. The perceived benefits of the higher priced proposal have to merit the additional cost, and the rationale should be well documented (from acquisition.gov[43]).

[40] https://www.gsa.gov/buying-selling/purchasing-programs/gsa-schedules/schedule-features/blanket-purchase-agreements

[41] https://www.gsa.gov/buy-through-us/purchasing-programs/multiple-award-schedule

[42] https://acquisition.gov/far/15.101-2

[43] https://acquisition.gov/far/15.101-1



Pre-negotiated Contracts

- Best for simple and commodity purchases
- Usually fastest and cheapest
- Limited flexibility

Lowest Price

- Best when requirements are well-defined and readily achievable
- Work well when when there is little differentiation between proposers

Best Value

- Best for complex systems and those with interdependencies
- Require justification
- Will usually be best for specialized election systems

8.2.1 Pre-Negotiated Contracts

Pre-negotiated contracts are typically the fastest way to make procurements, as terms and prices are already negotiated. State and local governments can usually buy off of their own state's schedules or the federal government's schedules, saving a great deal of time and effort. Because these agreements are typically negotiated for large quantities, prices are usually favorable.

Pre-negotiated contracts can be great if they meet exactly what you need (see the *Additional Resources* (page 56) section for federal resources for pre-negotiated contracts and a similar option provided by CIS through its CyberMarket[44]).

While efforts have been made to keep these contracts aligned with IT security needs, it's important to vet them for appropriateness in the election context—and ask an IT security expert if you need help. Note also that in some states, there are existing pre-negotiated contracts that may either drive toward a particular solution or in some cases require it. Most procurements of commodity IT, such as basic computer and server purchases, should be under a pre-negotiated contract.

[44] https://www.cisecurity.org/services/cis-cybermarket

8.2.2 Lowest Price and Best Value

When no item on a schedule meets the needs of the procurement, you need to conduct an independent procurement. There are two main types: lowest price and best value.

When you can clearly describe all of the requirements for a procurement, and multiple sellers can meet those requirements in similar and easily demonstrable ways, lowest-price procurements make the most sense.

For specialized procurements, best-value procurements are usually best. This will typically include hardware, software, or services that are specialized for elections. Similarly, risk mitigation in cybersecurity can be difficult to assess and describe before seeing a solution, so best-value procurements often lead to better security outcomes. Most procurements of election-specific IT should be conducted as best-value procurements.

Procurement offices sometime shy away from best-value procurements because of the difficulty many IT experts have in assessing the value of different solution features in financial terms. This can open the door for unfair decisions—whether actual or perceived—so procurement officers often require additional justification before allowing a procurement to go forward as best value. These justifications give confidence that the best-value determinations are made on an objective basis.

In making a justification for a best-value procurement, consider how you can describe incremental value associated with reaping additional benefits or eliminating risks. For instance:

- Is there other hardware or software that you'll no longer need to purchase because the more expensive option has a particular additional feature?
- Will the solution result in reduced operating costs due to fewer errors, provide for increased capabilities resulting in a greater portion of the job being done in an automated fashion, or result in the likely elimination of the need for other systems or staffing?
- Can you reduce risk (and consequently avoid cost overruns) because of the more expensive approach? If so, what is reducing this risk worth?
- What types of non-monetary value can you consider? Does a better security approach reduce reputational risk? Political risk? Can you estimate a range of financial value for reducing that risk?

The good and bad response descriptions in the best practices found in this guide can help with some of those justifications. Understanding these differing approaches to procurements—and being prepared to defend your rationale—can make or break a procurement. Above all, be prepared to be your own advocate for your needs.

Understanding these differing approaches to procurements—and being prepared to defend your rationale—can make or break a procurement. Above all, be prepared to be your own advocate for your needs.

8.3 Planning

The first step in a procurement is planning. It requires a clear understanding of the scope and objectives of the procurement, the requirements and desired outcomes from the procurement, and the risks associated with the procurement.

8.3.1 Define business objectives

Reviewing or defining the business objectives of the organization will help put the potential procurement in the context of the environment and will assist in many early, but critical, decisions. For the purposes of this guide, organizations should focus on their overall risk posture and the impact of potential unavailability or error in the individual functions and components of the election infrastructure. In addition, for IT procurements, clear objectives will help in the analysis of whether hardware needs to be purchased or leased, whether to use cloud or on-premises solutions, whether you need long-term sustained support or a surge of resources. The clearer these objectives at the outset, the higher the likelihood of a successful procurement.

Business objectives should be tied to organization outcomes that include expected benefits, acceptance criteria, success metrics, and financial impacts.

8.3.2 Draft requirements

The better the requirements for the procurement, the more likely you'll get what you want out of it. But the critical aspect is tying requirements of a product or service to the business needs of the organization. Requirements will identify deliverables and clearly indicate the requirements that must be met precisely and those for which a vendor may have flexibility to propose alternatives.

Election organizations might find that they need help defining requirements. They may look to requirements that have been defined by external organizations, such as the specifications developed by the EAC and NIST or contract requirements documents developed by other election organizations, some of which are listed on the EAC website. Some organizations may have a preference to reuse requirements from prior contracts.

The best practices provided in this guide can be helpful in identifying requirements that specifically address correctness of election IT functions and ensuring security of operations. It is recommended that the requirements include identification of minimum security requirements, where failure to provide results in disqualification, as well as desired security requirements, which can assist in ranking offerings from different proposers.

While requirements will evolve as you prepare for the procurement and gather additional information, it is still critical to develop them as completely as possible in this early stage.

8.3.3 Establish a procurement plan

Like anything, starting with a good plan will improve the chances of getting the outcomes you want. Using the objectives and requirements already established, you can develop a plan that includes timelines and identifies costs and risks.

At this stage, you'll often decide what type of procurement vehicle to use (e.g., sole source contracts, buying off a schedule, full and open competition) and will involve coordinating with procurement officials, business owners, and IT staff to ensure the plan is viable.

8.4 Market Research

Market research, including outreach to industry, can be an excellent way of identifying the functional and security capabilities that are available from other sources. The results of market research should serve as inputs to refining requirements. While a few voting machine vendors make up the vast majority of the market, the options for other systems used in election administration, especially those that run on commodity IT hardware and software, are as broad as the IT market as a whole. Thorough market research can ensure the procured items meet the desire outcomes.

Emphasis on security during market research is very important. Given the relatively recent increase in expectations regarding security, as well as the evolving threat to election systems, market research is an excellent opportunity to find out what industry leaders are doing with regard to security.

Moreover, market research helps identify some of the important differences between vendors that can impact outcomes down the road. Beyond the current-day capabilities, perhaps less exciting but as important are the service agreements, warranties, and lifecycle support differences that can have a long-lasting impact.

Quality market research can also help identify contract vehicle and discounting options, and can include working with other localities, the state, and even the federal government to obtain discounting and negotiated prices. Even if your locality can't take advantage of some of these opportunities, knowing about them can help you understand vendors' pricing structures and give you an advantage in negotiations.

One common way to perform market research is through a Request for Information (RFI) that is publicly posted or sent to potential vendors or contractors based on pre-defined criteria. Another popular method is to have an "industry day" that invites vendors to present to potential buyers. But conducting market research doesn't have to be entirely formal. Anything that increases your ability to make good procurement decisions—talking with colleagues about their experiences with vendors, searching for new vendors on the internet, making calls to vendors, reviewing past procurements and those from other jurisdictions—can all help you reach your goal.

Once you've completed your market research, you can update your procurement plan and requirements. With careful thought, planning, and research about what you need and what is available, you're ready to move on to the solicitation itself.

8.5 Solicitation and Award

Your jurisdiction may have specific requirements for which types of procurements it allows under a given set of circumstances, but generally you'll see that low-dollar value, short-lived, or commodity procurements don't require much scrutiny or paperwork, while large, long-lived, and specialized procurements have a longer lead time and require more review.

8.5.1 Issuing a solicitation

Simple procurements can be as straightforward as using a credit card or purchasing from a central buying office in your jurisdiction. The process is usually quite simple and isn't addressed in this guide. That said, improperly sourcing items as simple as a USB stick can have devastating security impacts. So even when it seems like a five-minute task, when it involves IT procurement, take all matters seriously.

For larger procurements, products and services are usually either purchased from an existing bulk contract or schedule or are solicited via a competitive procurement process. In the case of a procurement that requires highly specialized items or one in which there is only one vendor or a small number of vendors, remember that the security requirements don't change, and so the process for ensuring security shouldn't change even with limited options.

A Request for Quote (RFQ) or Request for Proposal (RFP) or similar tool triggers the formal proposal process. Once the RFQ has been released or published, the work of preparing the quote or bid is now on the vendor, but the government must still take an active part in the procurement. Widely circulating a procurement and being responsive to questions from bidders are critical aspects of ensuring strong bids.

8.5.2 Communication during solicitation

Maintaining fairness is important in the solicitation process, but so is maintaining communication. As with many processes, an all-too-common downfall of the solicitation process is a breakdown of communication between the government and vendors. In the interest of not divulging information that could unfairly advantage one vendor, government personnel sometimes shy away from answering questions or discussing the procurement with individual vendors. This can hinder a procurement and lead to proposers that misunderstand requirements or fail to properly reflect what is really important to the government.

Much of this can be avoided with good planning and research, but the government should also maintain communication throughout the process. A good—and inexpensive—way to answer questions while maintaining fairness is to require that all questions, with their answers, be posted publicly with the solicitation. Even with a proposers' conference, everyone will have access to clarifying information, which improves proposals and ultimately results in an improved outcome for the government.

Your state or locality may have specific rules or systems for questions and answers, so always work with the procurement authority to stay above board.

8.5.3 Evaluating proposals and selecting vendors

Evaluation of quotes or proposals should be a formal process to ensure the work that went into planning, researching, marketing, and clarifying the procurement goes to good use. Some IT procurements will choose selection of the proposal that has the lowest bid while meeting stated minimum requirements (lowest cost), while others will allow for a broader evaluation of all that is offered in the proposal (best value). Given the nature of security and the difficulty of capturing all security requirements as minimum, it is typically preferable to evaluate security using a best value evaluation method.

Whichever method is applied, evaluators should first eliminate any proposal that doesn't meet the minimum requirements. In a best value procurement, evaluators need to identify objective methods for identifying and assessing the value of additional attributes of a proposal when comparing it to a lower cost offering. When there are large differences in the proposals, it can be difficult to put a cost impact on the value of additional attributes, for example better security that may reduce the risk of successful attacks—which have very costly consequences. Critically important for a best value analysis is documentation and objective reasoning. Like everything, your jurisdiction's procurement rules matter, but, in general, documenting a defensible, objective basis for decisions will get the job done. Also, it is typically helpful to have one or more individuals not specifically involved with the procurement evaluation do an independent review of best value analyses to ensure that the logic behind the objective assessment is appropriately captured.

In best value procurements, negotiations are often part of the evaluation and selection process as well. Approaches to negotiations vary, but the government must go in with a clear expectation of what it wants and what it cannot accept. While no procurement is perfect, the clearer the expectations ahead of time, the higher the likelihood of a positive outcome.

8.6 Managing Procurements

Aside from the simplest of procurements, there is always more to it than delivery of a product and an exchange of money. For IT contracts in elections, this means that election officials and their teams need continual involvement in procurements, both from technical and non-technical personnel. This is true of all IT: hardware, software, and services, on-premises and in the cloud. To this end, individuals in election offices need a level of training that will enable them to understand what they can and cannot do in managing a procurement.

For hardware and software support contracts, IT and non-IT election staff should understand the service level agreements that were specified in the contract—who responds in an outage, what are expected uptimes, how quickly must a vendor respond to a system failure or other disruption. For services contracts, election staff should also understand contracted response times in case of emergencies, contingency plans, and how to enforce compliance in a critical situation. For many unexpected situations, someone whose day-to-day work is not in procurement likely won't have the experience or expertise to always have the right answer, so those individuals must maintain relationships with procurement officials.

There are a number of security focus areas that are important in managing contractors. In most cases, a contract will require a contract-specific security plan that outlines the processes and activities to ensure that security is maintained through activities such as security updates to software, vulnerability assessments, incident response, and personnel training. Keeping the procurement folks up-to-date on key activities, important upcoming events, and ongoing risks can speed their reaction time when something goes awry.

CHAPTER NINE

ADDITIONAL RESOURCES

- Belfer Center, Defending Digital Democracy Playbooks[45]: Guides to assist election officials and campaigns with improving their cybersecurity.
- Brennan Center for Justice, A Procurement Guide for Better Election Cybersecurity[46]: A look at seven key areas election officials and policymakers should consider as ways to achieve better vendor cybersecurity.
- CIS's CyberMarket[47]: CyberMarket is the CIS collaborative purchasing program that serves U.S. election organizations (among others) to improve cybersecurity through cost-effective group procurement. CyberMarket works with industry-leading cybersecurity providers to offer stakeholders access to training, software and applications, and services.
- CIS's Multi-State Information Sharing and Analysis Center[48] (MS-ISAC). The MS-ISAC works closely with election officials and security and technology personnel to provide the highest standards of election security, including incident response and remediation through our team of cyber experts.
- CIS's Essential Guide to Election Security[49]. A first-stop resource for election officials to learn about best practices in election security. This can aid the process of building a program designed to meet individual needs and abilities of any election office.
- CIS's Rapid Architecture Based Election Technology Verification[50] Program (RABET-V). A rapid, reliable, and cost-effective approach to verifying non-voting election systems.
- Election Audits, Readings and References[51]: Compiled for the 2018 Election Audit Summit at the Massachusetts Institute of Technology.
- CISA's Cybersecurity Toolkit and Resources to Protect Elections[52]. A toolkit including free tools, services, and resources provided by CISA, JCDC members, and others across the cybersecurity community.
- Federal Virtual Training Environment[53] (FedVTE): FedVTE provides free online cybersecurity

[45] https://www.belfercenter.org/project/defending-digital-democracy#!playbooks
[46] https://www.brennancenter.org/publication/procurement-guide-better-election-cybersecurity
[47] https://www.cisecurity.org/services/cis-cybermarket/
[48] https://www.cisecurity.org/ms-isac
[49] https://essentialguide.docs.cisecurity.org/en/latest/README.html
[50] https://www.cisecurity.org/elections/rabetv
[51] https://electionlab.mit.edu/election-audit-references
[52] https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections
[53] https://fedvte.usalearning.gov

training to U.S. government employees, federal contractors, and veterans. Through the MS-ISAC, U.S. election organizations can also gain access to FedVTE.

- The Institute for Public Procurement Document Library[54]: A library containing thousands of solicitations and templates, publications, and research to help you with your solicitation development activities.

- U.S. General Services Administration (GSA) Cooperative Purchasing Program[55]: With GSA's Cooperative Purchasing Program, state and local governments can get what they need—for less. The Cooperative Purchasing Program provides access to thousands of nationwide, pre-vetted vendors that offer a wide array of commercial information technology (IT) and law enforcement products, services and integrated solutions.

- The National Institute of Standards and Technology's Election Terminology Glossary[56]. Election terms including those used in the Voluntary Voting System Guidelines 2.0 (VVSG 2.0) requirements and glossary and in the NIST Common Data Format (CDF) specifications.

- Voting System Procurement Prep[57]: A vendor developed white paper, distributed at a National Association of Secretaries of State (NASS) conference, to assist state governments in making informed choices about procuring voting systems. White papers distributed at NASS conferences are not endorsed by the association, but simply made available to be shared with conference participants and Secretaries of State.

[54] https://www.nigp.org/home/find-procurement-resources/document-library
[55] http://www.gsa.gov/cooperativepurchasing
[56] https://pages.nist.gov/ElectionGlossary/
[57] https://www.nass.org/sites/default/files/events/2017%20Winter/Hart-white-paper-nass-winter17.pdf