CIS Center for Internet Security®

Managing Cybersecurity Supply Chain Risks in Election Technology

A Guide for Election Technology Providers

February 2021

Contents

Acknowledgments

CIS would like to recognize the following individuals and organizations for their support in creating this document. Their time and expertise were invaluable in completing this important work.

CIS Authors

Mike Garcia
Aaron Wilson

CIS Contributors

John Gilligan
Brian de Vallance
Curis Dukes
Phyllis Lee
Kathleen Moriarty
Lewis Robinson
Tony Sager
Ben Spear

Community Review and Contribution

Cybersecurity and Infrastructure Security Agency
Election Systems and Software
Hart InterCivic
Smartmatic
Unisyn Voting Solutions

In addition, CIS would like to thank the Democracy Fund for its generous support of this document's development.

1 Introduction

Since 2018, the Center for Internet Security® (CIS®) has produced several best practice documents as part of a comprehensive, nationwide approach to protect the democratic institution of voting and to manage the wide range of cybersecurity risks. These include:[1]

- *A Handbook for Elections Infrastructure Security*, developed to describe the general threats that exist in the election processes and establish a consistent, widely agreed-upon set of best practices to mitigate these threats.
- *A Guide for Ensuring Security in Election Technology Procurements*, to provide best practices specific to planning, developing, and executing procurements, including language that can be copied and pasted directly into requests for proposals, requests for information, and the like.
- *Security Best Practices for Non-Voting Election Technology,* to provide community-driven, comprehensive security best practices and implementation guidance for non-voting election technology to election officials and election technology providers.

This document continues our approach of providing best practices for specific problem areas identified to CIS by the election community. Officials and technology providers alike have repeatedly identified the need for guidance on managing supply chain risk to address the large proportion of election technology that is sourced externally. This document contains recommendations and best practices to address that need for cybersecurity risks, and refers to these other CIS documents to describe a holistic, consistent approach to risk management.

1.1 Audience and Purpose

The primary objective of this document is to provide election technology providers a mitigation approach for cybersecurity-based supply chain risks based on a risk assessment conducted by CIS. This document is intended to assist election technology providers in identifying the most significant cybersecurity supply chain risks for their products and choosing appropriate risk mitigation approaches for those risks.

Election officials may find the document instructive to understand how technology providers are going about managing their supply chain risk. In addition, Appendix C provides guidance for election officials to use when communicating with technology providers about supply chain risk.

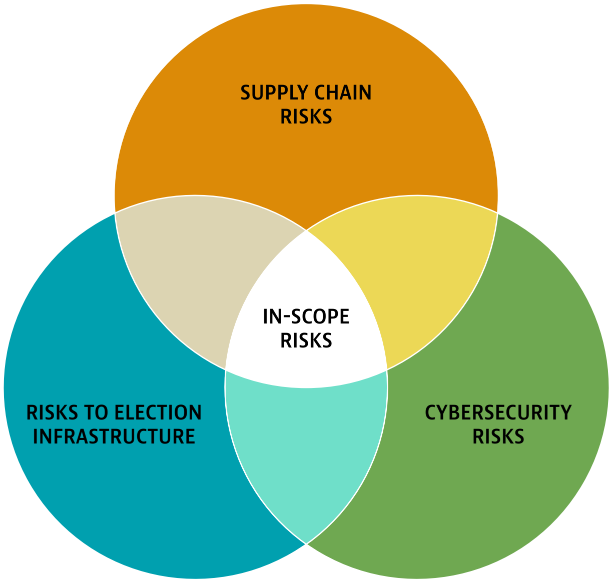
[1] For a complete list of CIS best practice products for elections, see https://www.cisecurity.org/elections-resources/.

2 An Overview of Cybersecurity in Supply Chain Risk Management

Not all supply chain risks are cybersecurity risks, and not all cybersecurity risks are supply chain risks. Moreover, some supply chain risks impact your products, while others impact your organization without directly impacting your products, such as an attack on your internal systems that may cause a delay in delivery, but doesn't alter or compromise any election product directly.

This document is tightly scoped to focus on supply chains and election infrastructure. Specifically, it is limited to risks that meet all three of the following conditions: 1) impact the supply chain, 2) are cybersecurity risks, and 3) have a direct impact on technology used in election infrastructure. The following Venn diagram shows the relationship of types of organizational risks; the center of the diagram is the scope of this document.

FIGURE 1. In-Scope Risks for *Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers*



Supply chain risk in this document refers to the hardware, firmware, and software sourced for use in election equipment. In addition to IT that ships with election equipment, it also includes externally sourced tools used to develop hardware and software in-house, such as software development kits, code libraries, information technology (IT) infrastructure, and the tools used to create, manage, and maintain that infrastructure.

2.1 Supply Chains

A supply chain is a network of organizations, individuals, resources, and information that, together, create and move a product or service to its final customer or end user. While this document addresses only IT activities and cybersecurity risks in election technology, supply chains also include physical, logistic, and financial activities.

For an election technology provider, all of the hardware and software developed outside the organization is part of its supply chain. Given that virtually all products contain components from outside the organization, one can safely assume that everything produced by an election technology provider is impacted by its supply chains. This includes the components that are used either inside a finished product or as part of its production process. Software development toolkits, workstations, removable media, and other technology used as part of the development process are still part of the supply chain.

Because of their physical nature, hardware supply chains are somewhat easier to identify and manage, though the extent and complexity of firmware has blurred the line between software and hardware, complicating the issue. Software supply chains often include both open source and proprietary code, commercial-off-the-shelf (COTS) products from large technology providers and highly specialized products, code that is purpose-built, and modules taken from online libraries. See Section 3.2 for more information on managing large COTS providers. Additionally, IT supply chains can have long lead times for substitution, a need for frequent updates, and sensitive compatibility issues.

Supply chains are a fact of modern life. No company develops everything itself, and nearly all IT used in election systems is sourced externally. As with IT in general, there is no reasonable way to eliminate all risk when sourcing externally. This creates an acute need for managing supply chain risk.

2.2 The IT Supply Chain in the Context of Elections

Managing supply chain risk is notoriously difficult. Organizations involved in large complex supply chains—from major retailers to the defense industry—struggle with appropriately making investments and accepting the risks that remain after these investments—known as residual risks. Smaller organizations often lack the resources to make appropriate investments and the leverage to influence their suppliers.

In elections, state and local procurement rules governing suppliers can complicate supply chain risk management, such as long lead times and blanket restrictions on the countries from which equipment can be sourced, however well-intentioned. Not all components of election technology are critical or carry the same risks, requiring a careful risk assessment of each component and a logical approach to mitigating it.

Rather than each election technology provider conducting a supply chain risk assessment on its own, this document serves as a resource to accelerate the process of developing or enhancing a supply chain risk management program. Most importantly, Section 5 provides a threat model for election equipment to assess the types of supply chain attacks election technology providers may face and will need to manage through their supply chains.

2.3 The Forward Supply Chain

In addition to managing your suppliers, some election technology providers need to consider forward supply chains—those organizations that take your products and provide them as a service or resell them. This is a common occurrence in elections and can present a risk to election administration using your products. To that end, assessing and managing downstream users of your products may prove a worthwhile investment for your organization and certainly for the integrity of elections.

3 Managing Cybersecurity Supply Chain Risk

Managing cybersecurity supply chain risk is a specialized aspect of an overall risk management program. The goal is to bring supply chain risk to an "acceptable" level, but determining what is acceptable can be as challenging as the mitigations themselves. This document can assist that process by providing the reader with a tailored assessment of risks and the identification of potential high-impact areas of vulnerability that will permit election organizations to focus on these areas.

Broadly speaking, election technology providers can significantly lower their supply chain risk by taking three approaches to manage cybersecurity risk:

1. A cybersecurity risk management program to address broad cybersecurity risks, regardless of whether they are supply chain risks
2. A supplier risk management program to reduce the risk from emerging threats and more elusive attacks
3. A targeted supply chain risk mitigation program for identifying and mitigating the most consequential supply chain risks associated with election equipment

This document briefly addresses the first and second approaches in this section and focuses on the third approach in Section 6. Appendix A contains more information on the second approach of developing a supplier risk management program.

3.1 Cybersecurity Risk Management

Managing cybersecurity risks is critical to maintaining a secure organization and secure products. All organizations should have some level of cybersecurity risk management program. Developing a unique program can be costly and time-intensive and a complete in-house assessment of IT risks is out of the reach of most organizations. Moreover, conducting such an assessment often yields results so similar to other organizations, it isn't worth the investment. Rather, organizations can build cybersecurity risk management programs through existing frameworks and controls developed through the experiences of many organizations and the input of many experts.

One good example is the CIS Controls®. The CIS Controls are organized into three Implementation Groups (IGs). Implementation Group 1 is considered basic cyber hygiene—a set of controls that provide effective security value with technology and processes that are generally already available. IG1 Controls don't exclusively address supply chain risks, but the risks they mitigate will help an organization address many common attacks. These are the table stakes of cyber defense and should be in place before taking additional steps toward a more comprehensive program.

Depending on the size and complexity of your organization, you may need to implement IG2 or IG3 as well. The CIS Controls provide a description of the organizations for which each Implementation Group is appropriate. After implementing IG1, organizations can conduct an assessment to determine if they need other Implementation Groups, whether in whole or part.

Prior work from CIS in the election space, including those referenced in the Introduction of this document, are built from the CIS Controls and align well with the Implementation Groups.

3.2 Supplier Risk Management

Managing suppliers is a critical aspect of mitigating supply chain risks. This is a five-step process:

1. Identify and document supply chain, including asset identification
2. Assess risks to prioritize critical components and services as those facing the most significant threats
3. Assess your relationships with suppliers relative to the criticality of products and services
4. Align and manage supplier relationships to manage risk
5. Conduct ongoing assessment and monitoring of key dependencies associated with critical components

The upshot of this process is to identify from whom you get things, ensure that you have the right type of relationship with them, and properly manage that relationship.

While this is a critical aspect of IT supply chain risk management, it is not the primary focus of this document. For that reason, details of establishing such a program are in Appendix A, with only a brief introduction here. The most important action for election technology providers is to assess the election-specific threat model described below and to adapt it to fit the needs of your specific organization or election systems.

Managing relationships with suppliers can be costly and time-intensive. There are several triggers for how concerned you need to be about your supply chain partners. Four important triggers are size, diversity, criticality, and customization. We'll briefly address these here and in more detail in Appendix A.

1. The size of suppliers has a large impact on the effectiveness of your monitoring. Larger firms will not give you the attention that smaller firms might. On the other hand, they are generally better resourced and will have more mature supply chain risk management programs in place. Smaller firms may grant you more access, but are likely more susceptible to attack, especially if they are a known supplier for elections. You should have higher expectations that large organizations can provide you with detail of their supply chain management practices on demand. You should plan to spend more time with smaller suppliers and directly investigate their security through site visits and close relationships. The location of a supplier should similarly affect your decision-making. For instance, a small supplier with little supply chain sophistication that is located in a costly—or impossible, such as during a pandemic—place to visit raises their risk to your organization.
2. The diversity of a supplier's customer base can also have a significant impact on how you manage the relationship. If they are known to supply election equipment, or only provide to critical sectors like defense and elections, they are of higher concern. If multiple election vendors source a particular component from the same supplier, that raises concern. Suppliers with a diverse customer base are generally of lower priority, but how they are used in your organization matters a great deal.
3. The criticality of a component to your products and operations can raise the importance of a given supplier dramatically. As with your own activities, you should invest more in products that are more critical to your operations.

4. The extent to which a component is custom-built for an election technology provider can add significant risk, even if it would otherwise be a trusted supplier. If aspects of the component, like firmware, are customized, you should consider more careful vetting.

While there are no hard rules that trigger a higher level of concern over a supplier, and they can sometimes be in conflict (e.g., a large supplier of a critical component), these triggers can help you prioritize limited resources. Still, they can't be addressed in isolation. Managing cybersecurity supply chain risk must be an integrated component of your overall supply chain risk management strategy, specifically as part of a defense-in-depth strategy to set up layers of controls throughout your value chain.

3.3 Resilience in Risk Management

In cybersecurity, bad things happen. Often what makes the difference is how you deal with them. Resilience is a hallmark of quality cybersecurity risk management. It reduces the consequences when an attack is successful by limiting damage and restoring aspects of an organization that were damaged or otherwise compromised.

Containers and virtual environments can limit movement across a network and facilitate quicker rebuilds to a known-good state without significantly impacting the efficacy of a production environment. They are particularly useful for remote connections.

Technology providers should also consider deploying "zero trust" architectures, which are gaining in popularity and provide an opportunity to limit the reach of a compromised component throughout a network. Broadly, zero trust architectures differ from perimeter-based defenses by using a model based on continual—or continuous—authentication measures for people, processes, and devices.[2]

[2] For more on zero trust architectures, see NIST SP 800–207 at https://csrc.nist.gov/publications/detail/sp/800–207/final.

Case Study: The SolarWinds Supply Chain Attack and Defense-in-Depth Security Strategies

Just prior to this document being finalized, the world learned of the SolarWinds supply chain attack. The consequences of this serious attack are not yet fully known, and likely won't be for some time. Because this document is focused on supply chain risk, this case study takes the viewpoint of an organization whose supplier has been successfully attacked, such as a customer of SolarWinds. It's worth mentioning, however, that as of this publication there is increasing evidence that SolarWinds itself was the victim of a developer tool supply chain attack, a major focus of this document.

The SolarWinds breach serves to underscore the importance of following the mitigation strategies in this document, reviewing and re-assessing your suppliers at regular intervals, and, even if a supplier is deemed trustworthy, verifying and monitoring their products prior to and during production.

The introduction of malicious code into the SolarWinds product was a particularly effective attack, as most network management systems are viewed as trusted and given significant access privileges to network and system components in an enterprise. Lessons learned from the SolarWinds attack will impact how organizations address such attacks on their supply chains.

While we currently believe there was limited or no impact on election infrastructure, this highly successful attack begs a question for all organizations deploying in complex IT environments: if a large, well-resourced supplier like SolarWinds can't prevent such an attack, how can I possibly keep these sorts of things from impacting my environment?

The answer, however unfortunate, is that there is very little most purchasers of the SolarWinds Orion product could have done to prevent the initial introduction of this vulnerability: they downloaded updates from a trusted site, installed signed and verified updates with valid hashes, and used the products as intended. SolarWinds has some 300,000 customers, including some of the largest organizations in the world. It supplies a wide range of customers in many industries. It meets both the size and diversity tests. Because of its size, an election technology provider would likely have no ability to impact SolarWinds's risk management practices, and would not be an influential customer in any respect. However, the criticality of some of SolarWinds's products could have a dramatic impact on an organization's operation.

Disheartening as this may seem, there is hope. You can't expect to catch or dissuade every possible attack—and you don't have to. You can implement security models that lower your risk even—especially—when facing the reality that some attacks will be successful.

There is evidence that the SolarWinds security model changed over time, including the physical locations at which critical work was conducted. Regularly updating assessments of suppliers can help identify some of these changes and, perhaps, alter your security posture toward them. You may also be able to negotiate for contract terms requiring notification of operational changes that impact your security, such as if operations begin in certain countries.

Risk is a function of the likelihood of something occurring and the consequences associated with it when it does occur. The supply chain mitigation measures discussed in this document serve to lower both the likelihood and consequence of successful attacks, but in general are geared toward avoiding them by lowering their likelihood of success.

On the other hand, at least with regard to supply chain attacks, the baseline cyber hygiene activities discussed above and the indirect mitigation measures in Section 6.3 can lower the consequence of an attack like the one against SolarWinds.

This is also where defense-in-depth comes in. While election technology providers should conduct supply chain risk management activities on these sorts of suppliers, you must assume that even the best defense measures will be imperfect. Defense-in-depth strategies refer to the layering of different risk mitigation approaches to stop attacks that might overcome any single hurdle. This increases the chance that, at some point, a threat actor will be tripped up and thwarted, or at least isolated to limit damage.

The logic for defense-in-depth is that no single defense is 100% effective, but together, a series of controls might come close. If supplier monitoring fails, product testing might catch it. If that fails, proper network segmentation might prevent an exploit's spread. If that fails, good access control might prevent significant exploitation of the vulnerability.

A good defense-in-depth strategy will thoughtfully implement controls of different natures to more thoroughly mitigate risk. This is, in essence, the idea behind control "families" seen in most major control guidance, like NIST Special Publication 800-53 and the CIS Controls. It also underscores the importance of implementing basic cyber hygiene to stop the most likely sets of attacks, then build upon that foundation.

4 Methodology for Election Supply Chain Threat Modeling

Threat modeling is a risk-based approach that is helpful in designing secure systems. It is based on identifying threats in order to develop mitigations to them. While you won't be able to eliminate all risks, threat modeling can be used to further prioritize efforts to mitigate the most significant of those risks.

The following threat model addresses attacks to the IT supply chain for election technology. It has been informed by analyses and experiences of CIS and its partners, including federal agencies, election officials, and election technology providers. It will work for most election technology products, but may need to be tailored for specific designs and implementations.

The threat modeling in this document is specifically for cybersecurity threats to IT, in the supply chain, that can directly impact election technology. First, we provide a set of attacker goals, describing the overall motivations of attackers. Next, we describe the expected threat space, a summary statement of the cyber threat actors and their goals based on prior evidence and future expectations. Third, we describe the most common attack types on supply chains, as well as other attacks that are sufficiently important to include here and are of particular importance for their contribution to a defense-in-depth model.

Finally, we provide an analysis of each election infrastructure component and the supply chain threats impacting them, along with mitigation approaches. This analysis is in Sections 5 and 6, respectively.

Section 5 provides the details of the analysis, while the remainder of this section describes how we built the election technology-specific threat model.

4.1 Attacker Goals

Cybersecurity professionals typically categorize attacks into three types of compromise: losses in confidentiality, integrity, and availability. These are the desired outcomes of the attack itself, independent of the attacker's motivation.

Motivation	Description	Attacker Motivation
Confidentiality	Exfiltrating intellectual property including source code and system designs, financial or personnel records, or sensitive election-related information such as voter records and ballot definitions	Low to Moderate
Integrity	Modifying information that can be used for strategic gain, such as modifying voter rolls or altering vote tabulation results	Moderate to High
Availability	Disabling an essential component of the election infrastructure, such as crashing websites and causing failures of e-pollbooks, ballot marking devices, or tabulation devices	Moderate to High

While losses in confidentiality may be a risk to elections and a motivation for attackers, the information gained from election technology providers is considered of lower value to an attacker when compared to risks from attacks on the integrity and availability—directly impacting votes or the ability to vote—and defamation—impacting the reputation of democracy and democratic institutions.

Losses of confidentiality would be beneficial to an attacker by later leveraging information gained, such as source code or design review notes, to perpetrate a later attack impacting integrity or availability. This would be a longer-term methodical sort of attack, which is common from nation state attackers. To that end, while likely lower in priority, threats to confidentiality should not be ignored.

Overall, the threat model focuses on the end goal objectives of likely attackers, and thus places emphasis on threats that impact integrity and availability.

Overall, the threat model focuses on the end goal objectives of likely attackers, and thus places emphasis on threats that impact integrity and availability.

4.2 Expected Threat Space

While overall threat space varies widely across the election environment, this document focuses only on supply chain threats. For instance, foreign influence is a major threat to elections in the United States, but foreign information operations (e.g., use of social media to spread disinformation) are not within the scope of this document because it is not a likely threat for the election technology supply chain. Information operations may be used for disinformation *about* supply chains, but are unlikely to be used as a direct attack *on* supply chains.

Based on experience since 2016 and analysis of potential attacker goals, we have determined that the highest risk of a supply chain attack comes from nation states attempting to compromise one or more elections, or to undermine confidence in U.S. elections in general.

The highest risk of a supply chain attack comes from nation states attempting to compromise one or more elections, or to undermine confidence in U.S. elections in general.

Cybercriminals, for instance, may attack election technology providers, but would likely do so with the same motivation as they would attack any other entity: seeking direct profit or valuable information. For this reason, election technology providers must be cognizant of cybersecurity threats they might face in their own organizations, such as ransomware attacks. While threats of this type are real and may impact providers, they are not supply chain attacks and election technology providers should be addressed as part of a broader cybersecurity risk management and defense-in-depth strategy.

Similarly, a nation state may co-opt or contract with cybercriminals to conduct operations, but if the nation state is the top-level threat actor, the motivations are that of the nation state, which drives the threat modeling.

Hacktivists may wish to disrupt an election through a supply chain attack, though for the purposes of affecting an election, the techniques they would use to do so will likely be the same as nation state actors, allowing us to keep focus on a single actor type.

For the remainder of the document, we focus on nation state actors that endeavor to alter or disrupt elections through the election infrastructure supply chain, or use such attacks to impact confidence in elections.

4.3 Common Attack Types

There are many ways to analyze and categorize supply chain attacks. In addition to general risks associated with COTS hardware and software, we define seven types of supply chain attacks that can be used by a nation state to sabotage elections:

1. **Development Tool:** deceiving a developer into using a fake or corrupted version of a development tool to introduce vulnerabilities into the code being developed
2. **Insider Threat:** infiltrating an organization through authorized access that is leveraged to conduct unauthorized and malicious activities
3. **Patch Site:** compromising a software update to introduce a vulnerability or prevent a vulnerability from being patched
4. **Source or Executable Code:** introducing vulnerabilities or replacing code with an illegitimate version in a direct attack on a product's code
5. **Download Site:** deceiving a user to download a fake or corrupt version of a product
6. **Backdoor Insertion:** manipulating hardware or software to allow access to a system that bypasses normal authentication procedures
7. **Third-Party Hardware/Firmware Corruption:** modifying the actual hardware or the software that is embedded in hardware to undermine integrity or cause component or system failure

These seven types of attacks will be used for defining the attack paths for each component of election infrastructure. Election technology providers should expect that a sophisticated threat actor like a nation state would employ multiple techniques to achieve its aims.

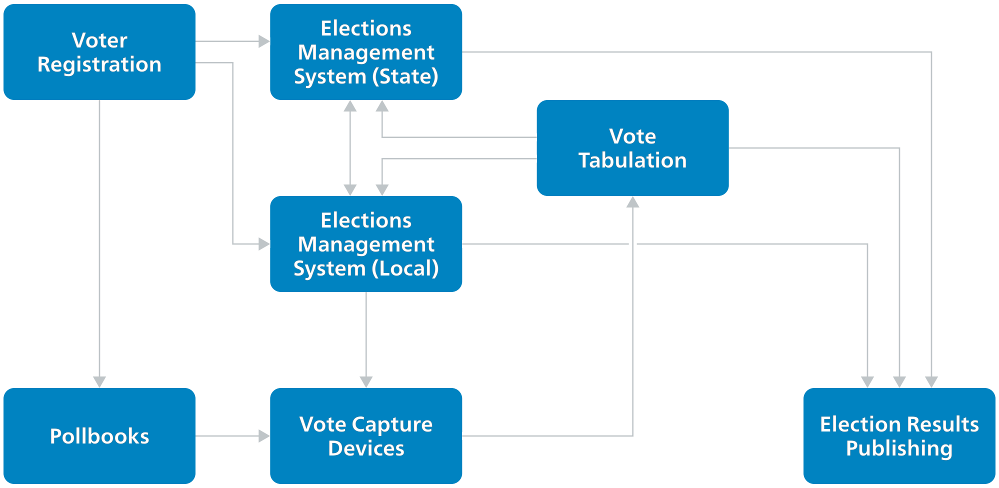
In addition, we identify multiple attack types that are not strictly supply chain attacks, but could be leveraged by threat actors as part of a broader attack and are significant enough to include here:

1. Channel Compromise
2. Authentication Errors
3. Network Vulnerabilities
4. Network and Interface Misconfigurations
5. Insecure Network Devices
6. Malware and Remote Execution
7. Denial of Service Attacks

Together, these techniques lead to our election supply chain threat model.

5 The Election Supply Chain Threat Model

This section iterates through each component of a generic election architecture first introduced in the CIS guide, *A Handbook for Elections Infrastructure Security.*


Voter Registration
Elections Management System (State)
Vote Tabulation
Elections Management System (Local)
Pollbooks
Vote Capture Devices
Election Results Publishing

For each component, we provide:

1. **Capability and Description:** each election infrastructure component is disaggregated into its primary IT capabilities (e.g., internal memory, networking) and has a description of each capability.
2. **Most Likely Attack Types:** each capability has a set of likely supply chain attacks. Adversaries generally take the least complex attack available to them; understanding these likelihoods is critical to targeting investments.
3. **Likelihood and Mitigations:** Each attack type has an assigned likelihood and has mitigations for the attack types. These likelihoods generally align with the risk ratings from the CISA Risk Prioritization Matrix.[3] Notably, because of different risk profiles within different components, similar capabilities (e.g., external memory) can have different likelihoods, even with the same attack types. We recommend beginning mitigation efforts with the highest risk capabilities.

After iterating through each of the election components, the mitigations to each of the supply chain threats are summarized in Section 6.

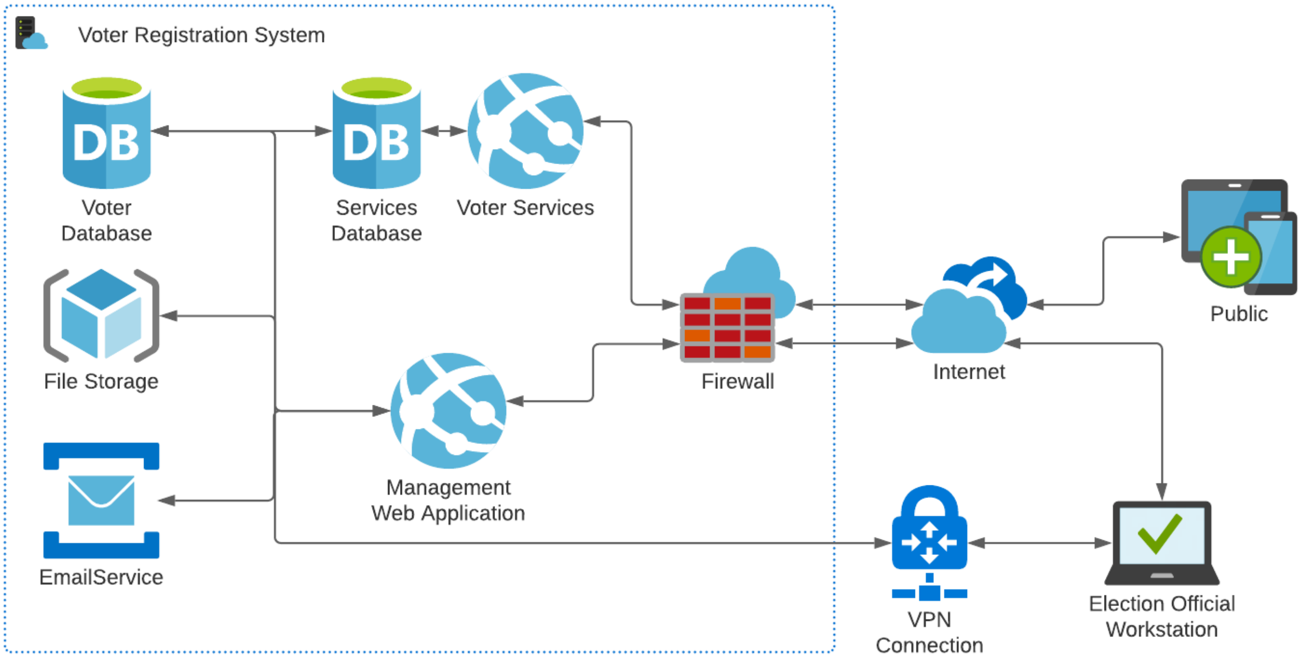
Remember, you as the election technology provider know your systems better than anyone else. What follows represents our best effort to provide actionable insights based on the generic architecture above and common deployments of each component. Your specific system architectures and deployments in election jurisdictions may differ from what's below, and you should assess our work as critically as you would anyone else's.

[3] See https://www.cisa.gov/publication/election-cyber-risk.

5.1 Voter Registration Systems

Voter registration systems provide voters with the opportunity to establish their eligibility to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks—paper and electronic—as well as provide information back to the voter as they verify their registration and look up polling locations. The functionality through a public portal varies widely, but the internal systems all provide these critical functions. Voter registration systems are typically dedicated software riding on COTS hardware and COTS operating systems.

FIGURE 2. A Typical Voter Registration System Architecture



The following table enumerates the capabilities of a typical voter registration system. For each capability, the table provides the most likely attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For voter registration systems, the highest likelihood is medium and it applies to software development and support, software attacks on internet-facing servers, software attacks on internal networks, attacks on external connections, software attacks on the voter registration database, and software attacks on registration database backup and replication.

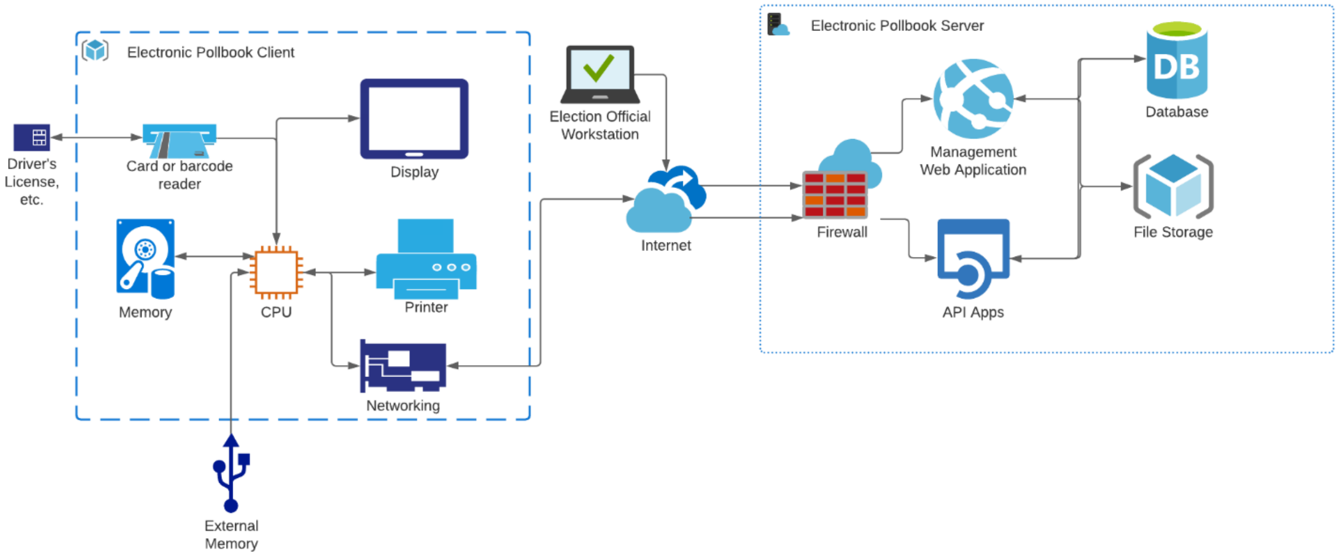
TABLE 1. Voter Registration System Capabilities, Attack Types, and Mitigations

Capability	Description	Most Likely Attack Types	Likelihoods and Mitigations
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting of personnel and components
Internet-facing server	Provides the interface to the public, including voter lookup, online registration or downloading of registration forms, and registration statistics. May have separate servers to perform some of these functions.	• Third-party hardware or firmware corruption	Low: • Follow vendor selection and assessment practices from Appendix A.
		• Insider threat, compromised developer tools, or modification of software	Medium: • Software verification • Configuration verification
Internal network	Used for managing and configuring servers and external connections, and for moving data from internal to externally facing databases.	• Third-party hardware or firmware corruption	Low: • Follow vendor selection and assessment practices from Appendix A.
		Corruption or misconfiguration through: • Compromised developer tools or modification of software • Source or executable code	Medium: • Network segmentation and dedicated network • Developer tool sourcing and validation • Software verification • Configuration verification
External connections (e.g., DMV, ERIC)	Connections with partners and data providers to share and collect information.	Software corruption or misconfiguration through: • Compromised developer tools or modification of software • Channel compromise • Authentication errors	Medium: • Network segmentation and dedicated network • Device allow-listing • IP, port, and service allow-listing • Standard security configurations • Identity management best practices
Voter registration database	Stores registration information for daily use and public exposure; this database may be part of a public-facing system.	• Third-party hardware or firmware corruption	Low: • Developer tool sourcing and validation • Vetting personnel and components
		Software corruption or misconfiguration through: • Compromised developer tools or modification of software or configuration	Medium: • Developer tool sourcing and validation • Software verification • Configuration verification
Registration database backup and replication	Copies of the voter registration database used for redundancy or restoration from backup.	• Third-party hardware or firmware corruption	Low: • Developer tool sourcing and validation • Vetting personnel and components
		Software corruption or misconfiguration through: • Compromised developer tools or modification of software or configuration	Medium: • Developer tool sourcing and validation • Software verification • Configuration verification

5.2 e-Pollbooks

Electronic pollbooks play a critical role in the voting process by providing functions such as ensuring that voters are registered and are appearing at the correct polling place, capturing a record of the voter having cast a ballot (but not what they voted for or against), and determining the ballot style the voter receives. Their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These e-pollbooks are typically dedicated software riding on COTS hardware and COTS operating systems.

FIGURE 3. A Typical e-Pollbook Architecture



The following table enumerates the capabilities of a typical e-pollbook. For each capability, the table provides the most likely attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For e-pollbooks, the highest likelihood is high and it applies to compromises of internal memory.

TABLE 2. e-Pollbook Capabilities, Attack Types, and Mitigations

Capability	Description	Most Likely Attack Types	Likelihoods and Mitigations
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting personnel and components
Input – Scanner	Conducts optical image scanning to capture driver's license or other forms of identification and transfers image to memory; typically configurable and contains firmware.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
		Forced misconfiguration through: • Patch site • Source or executable code • Download site	Low: • Configuration verification after delivery and updates
Input – Signature capture	Typically an external signature pad, though sometimes integrated directly to a touchscreen display.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
		Forced misconfiguration through: • Patch site • Source or executable code • Download site	Low: • Configuration verification after delivery and updates
Processing	The handling of the voter check-in process to produce a record of the voter's appearance at the polling station and assign the proper ballot to them.	Firmware or software corruption through: • Patch site • Source or executable code	Medium: • Firmware update or verification • Software verification • Firmware boot/runtime verification • Secure boot devices
Internal memory	Stores the voter records, to include information on eligibility, ballot assignment, and voting status. May require updates through a cloud or centralized system.	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing
Networking	Some systems require a network connection to conduct live updates; other systems do not have network capabilities or block connections.	• Network vulnerabilities and misconfigurations, insecure network devices	Medium: • Network segmentation and dedicated network • Device allow-listing • IP, port, and service allow-listing • Standard security configurations
Output – Paper barcode or ballot	Printed barcode used to activate a ballot marking device or an unmarked ballot.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
Output – Activation key	A digital certificate transferred to a smartcard that is used to activate the ballot marking device.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification

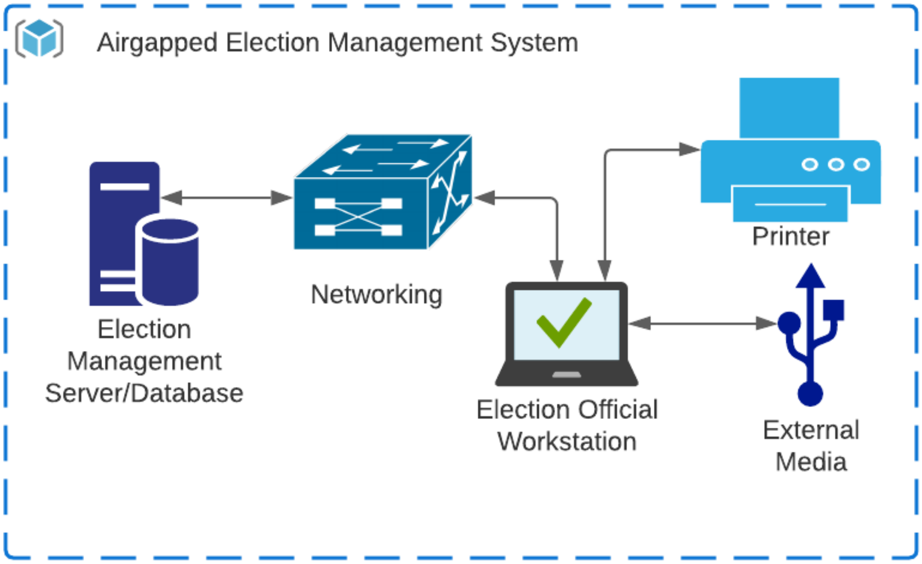
5.3 Election Management Systems

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. Jurisdictions have widely varying EMS functionality and use. For some states, local EMSs have no connection to state EMSs. Because of the air-gapping of these systems, we treat EMSs as distinct from each other.

Across jurisdictions, EMS configurations include a variety of functions. An EMS can conduct ballot design and generation, output machine configuration, and provide tabulation, aggregation, and reporting functions. Some functions are performed at the state level and some at the local level. Inputs may be as simple as a spreadsheet for programming ballots, but typically also include media devices containing votes and results for tabulation and aggregation. While an EMS may also include vote tabulation and election night reporting, in this document those functions are broken down into their own sections.

Due to the wide range of EMS activities, the analysis below may require more tailoring for a given jurisdiction than some of the other election components. As with all recommendations in this document, it's critical to understand why you're making the decisions you are and to be critical of them, even those coming directly from these tables.

FIGURE 4. A Typical Airgapped Election Management System Architecture


Airgapped Election Management System
Printer
Election Management Server/Database
Networking
Election Official Workstation
External Media

The following table enumerates the capabilities of a typical election management system. For each capability, the table provides the most likely attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For EMS systems, the highest likelihood is high and it applies to external media and input workstations.

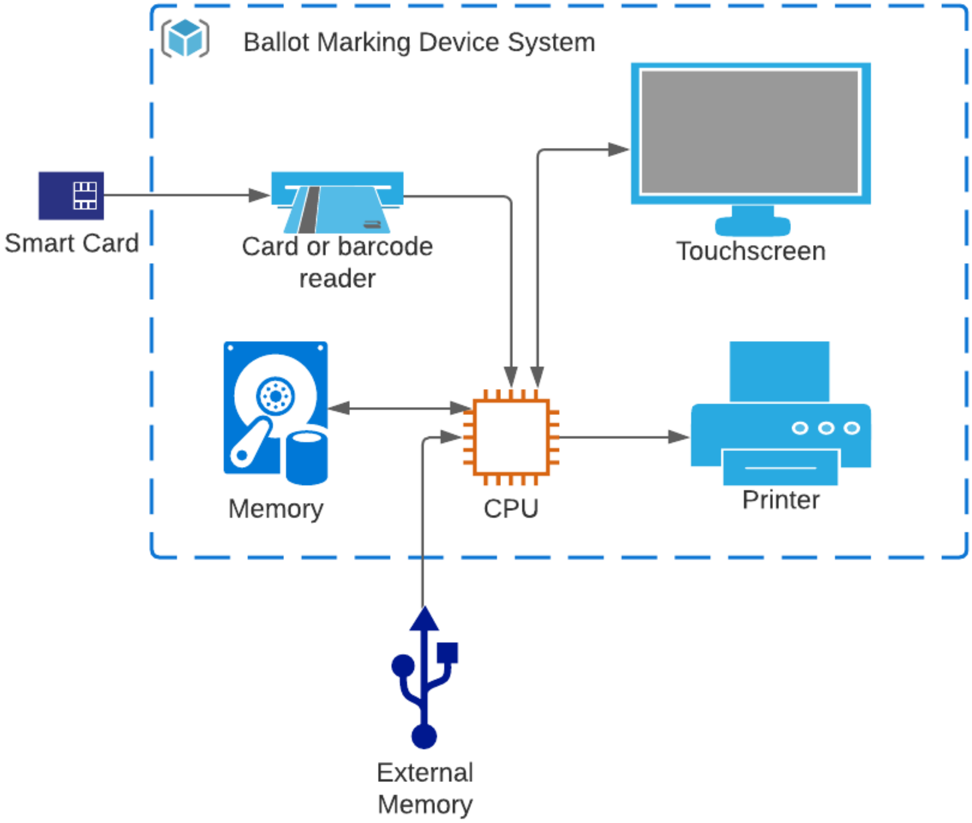
TABLE 3. Election Management System Capabilities, Attack Types, and Mitigations

Capability	Description	Most Likely Attack Types	Likelihoods and Mitigations
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting personnel and components
External media – All data input and output	In most deployments, the EMS is fully air-gapped and all digital input and output are exchanged through external media.	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing • Device allow-listing • No media reuse
Processing	Design and build ballots, program the election database, and conduct other critical election tasks.	Firmware or software corruption through: • Patch site • Source or executable code	Medium: • Firmware update or verification • Software verification • Firmware boot/runtime verification • Secure boot devices
Internal memory	Stores all information required for the election.	• Source or executable code	Medium: • Firmware boot/runtime verification • Strategic sourcing
Input workstation(s)	Because of the air-gap, EMS systems receive input either from one or more workstations via removable media or through a closed network in a server-client configuration.	• Source or executable code, malware, remote execution	High: • Dedicated workstations • Restrictive security configurations • Restricted use • Device allow-listing • No media reuse
Output – Printer	The EMS may print reports through an interface with a printer. This interface should be hardwired and will almost certainly be a COTS printer.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification

5.4 Ballot Marking Devices with Paper Outputs

This document focuses only on ballot marking devices (BMDs) with paper outputs; it does not consider hand marking or direct recording electronic machines. Most ballot marking devices receive the ballot definition, get activated by a key or code, display the ballot and allow the voter to make selections—typically through a touchscreen—and print out a cast vote record that is later tabulated. The ballot marking device does not store a record of the vote selections, only ballot accounting information (e.g., how many ballots were printed).

FIGURE 5. A Typical Ballot Marking Device Architecture with Paper Outputs



The following table enumerates the capabilities of a ballot marking device that produces a paper ballot. For each capability, the table provides the most likely attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For BMDs, the highest likelihood is high and it applies to processing and internal memory.

TABLE 4. Ballot Marking Device Capabilities, Attack Types, and Mitigations

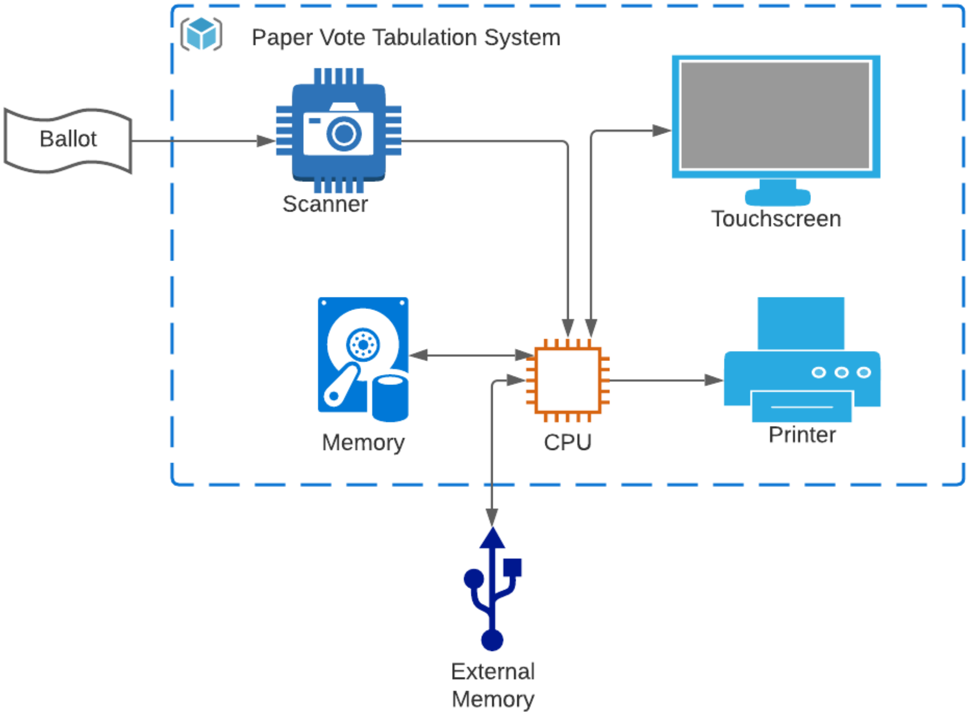
Capability	Description	Most Likely Attack Types	Likelihoods and Mitigations
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting personnel and components
Input – Activation key	A device, usually a card, that is used to activate the ballot marking device with the correct ballot definition for a given voter. Some keys, such as QR codes, use a scanner and avoid the threats posed by these connections.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
Processing	The handling of a voter's captured interactions with the ballot marking device to produce a marked ballot or cast vote.	Firmware or software corruption through: • Patch site • Source or executable code	High: • Firmware update or verification
		• Source or executable code	High: • Firmware boot/runtime verification • Secure boot devices
Internal memory	Stores the ballot definitions, the executables to control the equipment, and other data.	• Source or executable code	High: • Firmware boot/runtime verification • Digital signatures • Strategic sourcing
External memory	Loads election definition prior to equipment use; secondary storage for ballots and results on some types of machines.	• Source or executable code	Medium: • Firmware boot/runtime verification
Output – Human readable paper ballot	A ballot produced by the ballot marking device that displays the voter's choices in human-readable form.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
Output – Machine readable paper ballot	A ballot produced by the ballot marking device that shows voter choices encoded as a barcode or QR code.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification

5.5 Paper Vote Tabulation Devices

Supply chain threats to paper vote tabulation devices present significant risks. While most manipulation of vote tabulation results would be easy to detect through an audit, the risks still present a harm to elections by permitting altered reporting on election night. Even if later corrected in official results, an attack can achieve its goals by undermining voters' trust in the results and in elections in general.

Vote tabulation devices typically have multiple inputs and outputs, in addition to internal and external memory and processing capabilities.

FIGURE 6. A Typical Vote Tabulation Device Architecture



The following table enumerates the capabilities of a vote tabulation device. For each capability, the table provides the most likely supply chain attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For paper vote tabulation devices, the highest likelihood is high and it applies to processing, internal memory, and external memory.

TABLE 5. Vote Tabulation Device Capabilities, Attack Types, and Mitigations

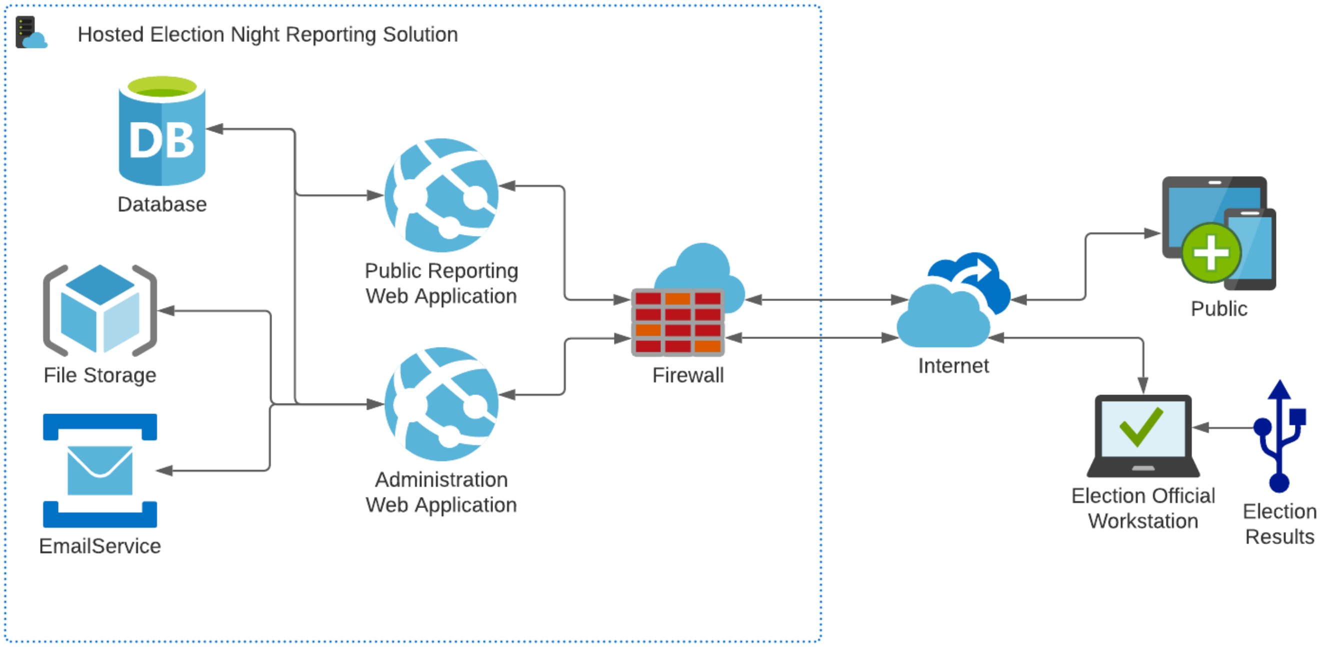
Capability	**Description**	**Most Likely Attack Types**	**Likelihoods and Mitigations**
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting personnel and components
Input – Scanner	Conducts optical image scanning of ballot and transfers image to memory; typically configurable and contains firmware.	Firmware corruption through: • Patch site • Source or executable code	Medium: • Firmware update or verification
		Forced misconfiguration through: • Patch site • Source or executable code • Download site	Low: • Configuration verification after delivery and updates
Processing	The internal computation conducted by the equipment; typically contains hardware, firmware, and software.	Firmware or software corruption through: • Patch site • Source or executable code	High: • Firmware update or verification
		• Source or executable code	High: • Firmware boot/runtime verification • Secure boot devices
Internal memory	Stores copies of each ballot, the executables to control the equipment, and other data.	• Source or executable code	High: • Hardware and firmware verification • Digital signatures • Strategic sourcing
External memory	Loads election definition prior to equipment use; secondary storage for ballots and results.	• Source or executable code	High: • Device allow-listing • Digital signatures • No media re-use • Strategic sourcing
Output – Printer	Prints aggregated results of scanned ballots; typically contains firmware.	Firmware corruption through: • Patch site • Source or executable code	Low: • Firmware update or verification
Output – Display	Displays various information based on equipment: a running count of scanned ballots, an image or the results of the last scanned ballot, or the aggregated results; typically contains firmware.	• Patch site	Low: • Firmware update or verification

5.6 Election Night Reporting Systems

While election night reporting (ENR) systems are only used for unofficial results, these are the results that shape the world's impressions of American elections. For that reason, it is critical that they are available to the public as expeditiously as possible and very closely reflect the official results that will follow.

ENR systems input tabulated votes, aggregating and formatting them as needed, and outputting results in various formats (e.g., XML, HTML, PDF, CSV) through a website or application programming interface (API). This can occur in several ways. A common one is with a local EMS as an intermediary, taking tabulated results and producing a report that is used by the ENR to aggregate results across the state, publish them to a website, or populate an API feed. Whatever the implementation, the systems used for reporting and publishing are likely networked and, in many cases, have public-facing websites. There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results may be kept on a system that is not persistently connected to the internet.

FIGURE 7. A Typical Election Night Reporting System Architecture


Hosted Election Night Reporting Solution
DB
Database
File Storage
EmailService
Public Reporting Web Application
Administration Web Application
Firewall
Internet
Public
Election Official Workstation
Election Results

The following table enumerates the capabilities of a typical election night reporting system. For each capability, the table provides the most likely attack types, the likelihood of that attack occurring, and the approach to mitigating the risk of the attack being successful. For ENR systems, the highest likelihood is high and it applies to internal memory.

TABLE 6. Election Night Reporting System Capabilities, Attack Types, and Mitigations

Capability	Description	Most Likely Attack Types	Likelihoods and Mitigations
Software development and support	A general aspect of the equipment build; this includes the tools used to develop the hardware, software, and firmware that is part of the equipment.	• Compromised developer tools or modification of software, firmware, hardware	Medium: • Developer tool sourcing and validation • Vetting personnel and components
Input – Tabulated results	Results from the various tabulators; typically input through external memory, such as a USB drive.	• Source or executable code	Medium: • Device allow-listing • Digital signatures • No media re-use
Processing	Aggregating of tabulated results and formatting for reporting to the central reporting authority.	Firmware or software corruption through: • Patch site • Source or executable code	Medium: • Firmware update or verification
		• Source or executable code	Medium: • Firmware boot/runtime verification • Secure boot devices
Internal memory	Local storage of tabulated results and aggregated results report. This may be local, central, or cloud storage.	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing
Networking	Network connections from local reporting to central reporting. This is typically done through SFTP, VPN, or secure web connections.	• Network vulnerabilities and misconfigurations, insecure network devices	Medium: • Network segmentation and dedicated network • Device allow-listing • IP, port, and service allow-listing • Standard security configurations
Output – API feeds	Data connections from external sources, such as API feeds used for reporting to media organizations and the public.	• Interface misconfiguration, denial of service attacks	Medium: • Deploy API management
Internet-facing server	Provides the interface to the public with unofficial results.	• Third-party hardware or firmware corruption	Low: • Follow vendor selection and assessment practices from Appendix A
		• Compromised developer tools or modification of software	Medium: • Developer tool sourcing and validation • Software verification • Configuration verification

6 Mitigation of Specific Election System Risks

The election technology threat model described in the prior section is intended to serve as a roadmap for risk mitigation by election vendors. Election technology providers can benefit from the collective insights and experience of the threat model to help identify the priorities for their risk mitigation efforts as well as candidate approaches to mitigate these risks.

The attack types in the tables in the preceding sections have known mitigations, as shown in the Likelihoods and Mitigations column. This section lists those mitigations, describing them and the approach to implementing them.

In addition, Section 6.3 lists a number of other mitigations that do not appear in the tables above, recognizing that it is impossible for any one approach to stop all exploitations. As part of a quality overall cybersecurity posture, and in support of a defense-in-depth strategy, the non-supply chain mitigations in this section are the most beneficial to thwarting supply chain attacks when they make it through to your systems.

6.1 Prioritizing

As mentioned early in this document, all organizations need a baseline of cyber hygiene to have any hope of effective cybersecurity risk management. With this in place, election vendors should put initial priority on mitigation of those risks that have a high or medium likelihood before addressing risks that are identified as low likelihood. Just prior to each of the tables above, we list the highest risk capabilities of each components; we recommend these be the priority in developing a program to manage cybersecurity risk in your supply chain. They are also summarized in this section.

TABLE 7. Summary of High Likelihood Attack Types

Component	Capability	Most Likely Attack Types	Likelihoods and Mitigations
e-Pollbooks	Internal memory	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing
EMS	External media – All data input and output	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing • Device allow-listing • No media reuse
BMD	Processing	Firmware or software corruption through: • Patch site • Source or executable code	High: • Firmware update or verification
		• Source or executable code	High: • Firmware boot/runtime verification • Secure boot devices
BMD	Processing	• Source or executable code	High: • Firmware boot/runtime verification • Digital signatures • Strategic sourcing
Tabulation	Processing	Firmware or software corruption through: • Patch site • Source or executable code	High: • Firmware update or verification
		• Source or executable code	High: • Firmware boot/runtime verification • Secure boot devices
Tabulation	Internal memory	• Source or executable code	High: • Hardware and firmware verification • Digital signatures • Strategic sourcing
Tabulation	External memory	• Source or executable code	High: • Device allow-listing • Digital signatures • No media re-use • Strategic sourcing
ENR	Internal memory	• Source or executable code	High: • Firmware boot/runtime verification • Strategic sourcing

For some election technology providers, you may need to make decisions about which products to prioritize. “All of them,” unfortunately, is not always a viable answer in a resource-constrained environment. In addition to considering the likelihood of attacks on particular capabilities, you’ll want to prioritize actions that will have the greatest overall impact on your organization, such as components that are used across all of your products. Another consideration is whether newer or widely distributed products might have priority over products near their end-of-life.

Having sufficient knowledge of your operations is vital to determining the priority of products; priority should be backed up with analysis, be deliberate, and be defensible.

6.2 Direct Supply Chain Mitigations

The following mitigations will directly reduce supply chain risks and should be implemented as indicated in the tables above. There are sources for security best practices for these mitigations, to include the CIS Controls, the NIST Cybersecurity Framework, and NIST SP 800-53.

Developer Tool Sourcing and Validation

- Most development tool risks can be mitigated by choosing these tools carefully; lesser known and free tools may be less secure or contain backdoors.
- Tool approval should be an organizationally-managed effort; blocking use of tools not specifically reviewed or approved avoids risks like typosquatting or engineers hastily choosing a tool.

Vetting Components

- Component vetting can include logic and accuracy testing, confirming digital signatures, physical inspection, and other procedures that increase confidence that the component works as intended.
- This should also include finished product testing, such as quality sampling off the production line.
- Risk management procedures can include quality checks at later points in the supply chain or production process, as long as they recognize that detecting malicious acts after the fact is quite difficult.

Firmware Update

- Firmware updates should be received directly from the manufacturer through physical media or a signed, trusted update site.
- Updating firmware with verified code mitigates the risk that it was intercepted and modified later in the manufacturing process or during shipping.

Hardware and Firmware Verification at Boot and Runtime

- Also known as hardware attestation, a firmware version can be validated through the checksum hash against manufacturer published records.
- These measures mitigate the risk that the firmware was modified after its development by the manufacturer. To determine whether the manufacturer develops its products safely, use the practices for assessing supplier relationships in Appendix A, Section A.4.
- Increasingly, hardware providers offer firmware verification during runtime in addition to at boot. Older equipment may not support this, but newer hardware should and, if it does, attestation should be part of ensuring a trustworthy runtime environment.

Software Verification

- Software can be verified and validated in a variety of ways, but should include both static and dynamic methods as a part of the software development process.
- Robust software verification, including comprehensive testing, can address many risks both within and outside of the supply chain.

Configuration Verification

- Verify the configuration of equipment by manually comparing it to a documented configuration.
- Verify the review through a logic and accuracy test.

Verified or Secure Boot

- During the boot process, verify the authenticity of each subsequent step in the process before handing over control. Many hardware systems provide a secure boot capability.
- When building equipment, instantiate a verified or secure boot process to include rollback protection into the boot manager.
- All firmware components must be properly signed.

Strategic Sourcing

- Sourcing from trusted or well-managed resources can reduce the risk of supply chain vulnerabilities.
- Follow the practices in Appendix A of this document, as well as applicable best practices in *A Guide for Ensuring Security in Election Technology Procurements*.

6.3 Security Best Practices Indirectly Mitigating Supply Chain Risk

It's impossible to eliminate all supply chain risks. The best practices listed below do not mitigate supply chain vulnerabilities before they are introduced to an organization's assets but, when implemented as part of a broad cybersecurity risk management program, help mitigate residual risks that may exist even in the face of an effective supply chain risk management program.

Access Control

- **Personnel:** For critical components, personnel that work along the supply chain and with end products should have at least a national agency check and either be U.S. citizens or, if not U.S. citizens, be subject to additional risk management procedures.[4] Personnel security measures should be deployed to include this vetting and continual monitoring for changing circumstances and suspicious behavior. This should apply to employees and contractors.
- **IT environments:** Some best practices, such as rapidly deploying patches, can have unintended consequences, for instance if the vendor issuing the patch is compromised. This is *not* a reason to forego the best practice, but rather to execute it wisely through a defense-in-depth strategy. Access control mitigations, such as monitoring for uncharacteristic behavior by user account and sudden changes in user privileges, can help mitigate the consequences of zero-day attacks and other vulnerabilities that enter your environment.

Configuration Management

- Configuration management is wide ranging and includes controlling the process for changes to any asset in an environment.

[4] For more information on national agency checks, see https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

- Establishing a robust configuration management process is one of the most effective measures to limiting damage from vulnerabilities. Malicious software or hardware components that make their way into an environment can be identified or stymied by quality configuration management.
- Processes should be developed and reviewed to systematically manage, organize, and control changes into an environment, including documents, software, hardware, testing processes and documentation, and other assets during the development lifecycle and as part of updates and modifications to existing components.

Network Segmentation

- Segmenting networks can minimize the risk of malware on an infected device from crossing laterally from compromised network resources to others.
- Follow Best Practice 6 of *A Handbook for Elections Infrastructure Security*.

Identity Management Best Practices

- Identity management best practices are well documented, but should include the following: use of multi-factor authentication, providing the least privilege necessary to users, and removing stale accounts.
- Election technology providers should validate that these best practices are used throughout the entire supply chain.
- Follow Best Practices 24–26, 47, and 49–53 of *A Handbook for Elections Infrastructure Security*.

Allow-Listing: IP, Port, Service, and Device

- While allow-listing and other network management approaches do not directly reduce supply chain risks, they can help mitigate any supply chain vulnerabilities that have not been addressed elsewhere.
- Follow Best Practices 1–3 of *A Handbook for Elections Infrastructure Security*.

Standard and Restrictive Security Configurations

- Creating and maintaining standard configurations for devices can eliminate unexpected vulnerabilities that stem from misconfigurations.
- While devices should use standard configurations wherever possible, there can be more than one standard, including one for devices that should have highly restrictive configurations that limit their functionality.
- See Best Practices in Section 1.3 of *Security Best Practices for Non-Voting Election Technology*.

Dedicated Workstations

- Consistent with using restrictive security configurations, some systems, particularly those used to exchange data with non-networked or air-gapped systems (usually via removable media), should have a configuration that permits only the critical task or tasks necessary to exchange that data; all other functionality should be removed from the system (preferably) or disabled if removal is not possible.

Single Use or Sanitization of Removable Media

- Discarding removable media after a single use will not eliminate supply chain risks associated with removable media—if the media arrived in a compromised state, any malware will likely be deployed on the first use. That said, removable media is a common vector for spreading malware across systems, especially systems that are not directly connected to the internet.
- To that end, limiting most removable media to a single use is still an important supply chain risk mitigation for the most critical systems.
- For some jurisdictions, single use of media will prove cost prohibitive for all systems. While still the best practice, an alternative is to use sanitization tools for all removable media. There are many guides and commercial tools to assist in this process.
- Additional controls include encryption to limit exposure of data and drive locking to prevent introduction of unauthorized media.
- See Best Practice 63 of *A Handbook for Elections Infrastructure Security* for single-use media and NIST SP 800-88 for guidance on sanitization.

Digital Signatures

- Digital signatures provide an assurance that data that have been signed have not been tampered with since that signing.
- Digital signatures can help mitigate tampering risk for a variety of data, including firmware and software code, configuration data, and election results data.

API Management

- API vulnerabilities can stem from provisioning, management, and orchestration activities. Vulnerabilities can be introduced anywhere along the supply chain and exploited once the API is live, but whether the vulnerability is intentional or due to a misconfiguration, proper management during deployment and operation can mitigate most risks.
- APIs are also typically the most exposed part of the system as they live outside the organization’s trusted boundary.
- APIs should be validated as operating properly (e.g., accepting only the correct information and handling erroneous inputs properly). API’s that are not necessary for the functions being supported should be disabled or removed.

Training and Education

- Just like other cybersecurity risks, everyone in your organization should have a basic understanding of supply chain risks. Good training regimes can raise awareness and improve overall outcomes, augmenting the more formal efforts described throughout this document.

7 Communicating Your Supply Chain Risk Management Approach

Anticipate that you will be asked to describe your supply chain risk management approach, both publicly and as part of procurements by election officials. To that end, you should have a communication plan and documentation for addressing questions.

Your communication plan does not need to be extensive or reveal every detail of your and your suppliers' approaches. It should, however, provide broad answers to common questions.

- Your plan should describe your basic approach, including adherence to any standards or public guidance.
- It should describe the methods you use to assess your suppliers: site visits, testing, documentation reviews, questionnaires, etc. If you are not comfortable revealing a general description of approaches you do (and don't) take, then perhaps you shouldn't be comfortable with the level of risk they are (or aren't!) mitigating.
- Be ready to provide information on the geographic sources of the hardware and software you procure. Even if you are comfortable with the approach you take to managing these risks, you need to be ready to talk about it in a way that makes others comfortable.

In procurements from election organizations, you may be asked for more detailed information. Having a well-documented supply chain risk management program and carefully maintaining the results of our various assessments will allow you to quickly provide the level of detail needed. Expect to be asked how you are addressing the high-likelihood items in this document, as well as how you are prioritizing the development and evolution of your cybersecurity supply chain risk management program. Our procurement guide, *A Guide for Ensuring Security in Election Technology Procurements,* and the information in Appendix C can provide a more detailed understanding of what you should expect from election officials.

Communicating about your plan should not be a strictly defensive measure that is triggered when you get questions or an incident occurs. It is an active part of risk mitigation—it helps manage communications and reputational risk.

Cybersecurity risks do not live in isolation from one another or from other types of threats, such as physical attacks. Supply chain risks will inevitably be used as a foil for information operations. Communication risk management should work with technology risk management to address both reactive measures—responding to misinformation about the security or election technology—and proactive measures—educating election officials, the media, and the public to build trust.

8 Conclusion

You cannot expect to eliminate all cybersecurity risk in your supply chain. The best you can do is be informed regarding the most significant supply chain risks, proactive in applying mitigations, and responsive to changes. Doing this requires understanding your environment and how your suppliers impact it, establishing a meaningful supply chain risk management program, evolving and maturing that program over time, and coupling it with effective cyber hygiene within your organization.

Following the guidance in this document will help you achieve those ends, both through the specific threat identification and mitigations for election infrastructure and through the guidance for developing and implementing a program to manage your suppliers. With limited time and resources, you'll need to prioritize mitigations. Begin with the most significant risks and, as resources permit, continue with remaining risks.

Over time, as you manage cybersecurity risks in the election technology supply chain, the threats will change and so must your mitigation strategies. As you take this document and shape it into your own supply chain risk management program, expect to revisit it, update it, and continue to evolve and stay ahead of threats to your supply chain.

Appendix A: General Information on Supply Chain Risk Management

There are several resources for IT supply chain risk management guidance. One of the most comprehensive is NIST Special Publication 800-161 (NIST SP 800-161), Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST SP 800-161 provides guidance to federal agencies on identifying, assessing, and mitigating IT supply chain risks at all levels of their organizations. Many organizations, especially smaller ones, might find NIST SP 800-161 overwhelming. This appendix provides streamlined guidance to managing suppliers, though it does not provide a control set overlay in the way NIST SP 800-161 does.

If your organization finds the mitigations in the main body of this document, along with the CIS Controls, insufficient, you may find the controls in NIST SP 800-161 valuable for managing your supply chain risks that are not found in this document. These controls are based on NIST Special Publication 800-53, which may be familiar to IT security professionals.

Prior to using those resources, we recommend that election technology providers review this appendix and, if necessary, consult NIST SP 800-161 for additional controls and details.

A.1 Process of IT Supply Chain Risk Management

The remainder of this appendix addresses the five-step process introduced in Section 3.2:

1. Identify and document supply chain, including asset identification
2. Assess risks to prioritize critical components and services as those facing the most significant threats
3. Assess your relationships with suppliers relative to criticality of products and services
4. Align and manage supplier relationships to manage risk
5. Conduct ongoing assessment and monitoring of key dependencies associated with critical components

To reasonably manage risk, each of these steps is necessary. Steps 1 through 4 should occur as a recursive process of improvement, while step 5 should be a continual aspect of operations. Each of the steps is detailed to provide an ability to initiate or enhance a program to manage cybersecurity supply chain risk in your organization.

A.2 Identify and Document Your IT Supply Chain

There are many approaches to developing a detailed understanding of your supply chain, and multiple approaches may be necessary to capture the entire supply chain.

You likely maintain a product component inventory, bill or materials, or the like. Compiling a full supplier list for all products will go a long way toward completing step 1. These bills of materials exist for both hardware and software. As the supply chain can be complex, this begins with carefully analyzing each aspect of your organization and how it is supplied.

For most internal-use workstations, servers, peripherals, and removable media, the most direct approach to building a list of suppliers may be to work with your procurement or accounting team to develop a list of ongoing contracts and purchase records for active hardware, software, and services, such as purchase card receipts. Your IT team should maintain an inventory of assets that can be leveraged to build a full supplier inventory.

With this list, you'll want to build a spreadsheet or database of all the items supplied, who supplies them, and the type of relationship you have with each supplier (e.g., contract, simplified purchase, service). Capture other important information about the item and supplier, like how critical it is to your organization's processes, when in those processes it's needed, how often it's procured, when the contract expires, and whether any individuals require ongoing physical or logical access, such as to make changes or updates.

A.3 Assess and Prioritize Products, Services, and Components

The second step involves understanding the criticality of each procured or externally sourced aspect of your products, services, and components. With the results of a threat model, or using the one provided earlier in this document, you can align your IT supply chain management efforts to focus first on the most significant threats faced within election systems. Aside from leveraging the threat model in the main part of this document, you can consider some of the following questions to assess whether a product, service, or component carries significant supply chain risks. Remember that this part of the assessment is about the product, not the supplier:

1. Could the item pose a risk to safe, secure, fair elections?
   - Pencils likely don't, servers could.
2. Could an error or malicious effort cause a severe disruption to the election or undermine confidence in the results?
   - This should be taken broadly; undermining confidence should be considered as serious as actual impact to the election.
3. Could the supplied item be a target because it is specific to elections?
   - If you're buying a product that is used in many industries, the likelihood of a specific target is lower.
4. Are there perception risks to consider?
   - Even if technical risks are well managed, trust and reputation matter a great deal. Managing—or an inability to manage—communication and reputational risks may impact decision-making.

Threat modeling is a tedious process and requires a fair amount of dedicated time and specialized expertise. Answers to these questions could add or remove risks from your threat model. After making any necessary adjustments, it's time to begin taking action to mitigate risk.

A.4 Assess Your Supplier Relationships

Suppliers that have been prioritized as providing critical components—which includes portions or all of the hardware and software components in your products and also the tools used to develop the products—can have an outsized impact on the security of your organization. If they are a known supplier for your election technology, that informs a potential adversary that they are a vector for attacking you. For this reason, it's important to strategically analyze those relationships and manage them accordingly. The next section provides more details on relationship types.

You can also learn a great deal through information sharing mechanisms. These can be formal such as through the EI-ISAC and Sector Coordinating Council, or informal through relationships with other election technology providers, election officials, and other partners.

A.4.1 The Basic Questions

Consider some of the following questions as you review each supplier relationship:

1. What is your relationship with the supplier?
   - Does the supplier make site visits or have you met in person?
   - Does the supplier have an appreciation for the threat landscape? Does it face the same threats?
2. Does the supplier know what business you are in and how your products are being used?
   - In some cases it's better that a supplier understands the end product. In other cases it's better to maintain an arms-length relationship.
   - Try to avoid the "space in between." If the supplier knows its products are going into election technology, you need to understand more about their security posture. If the supplier doesn't know that and its products are distributed widely, you can maintain more of an arms-length relationship.
3. What does the supplier's supply chain look like? What is its approach to supply chain risk management? What procedures and controls are in place by the supplier to reduce risk in its supply chain? Does the supplier provide an audit attestation to support its policy and procedures are as expected?
   - If it is producing election-specific products—or knows that you are—the supplier needs a more mature approach to supply chain risk management.
   - If its products are integrated in critical aspects of the election process, the supplier needs a more mature approach as well.
   - IT is seldom produced wholly in the United States. The supplier should know from which countries it accepts components and whether foreign-sourced components will require additional testing or verification.
   - Ownership and location of facilities matter. Require the supplier to provide this information and make risk-based decisions, especially when known adversary states are involved.
4. How big of a vendor are they? Do you have influence over them?
   - Large vendors are likely diversified beyond elections and are more likely to have mature approaches to supply chain risk management. But they should also be able to demonstrate this.
   - Increasingly, large vendors are taking special care with election products. Ask if they have additional security measures available to you.
   - Small vendors may require more scrutiny to ensure they are taking a sound approach to security internally and with their own suppliers.

- Regardless of size, it's also important which types of industries the vendor supplies. The more sensitive industries they supply, the more you'll need assurance of their supply chain practices.

A.4.2 A More Detailed Assessment

Good suppliers, even smaller ones, will be able to answer questions about their security practices and supply chains—just as you should be able to answer questions from election officials.

Appendix B contains an additional set of questions you should be asking. Some may not be applicable, but together they will give you significant insight into how the supplier functions. The questions are organized into three groups addressing different aspects of the supplier's approach: organizational, internal policies and practices, and supply chain practices. You can use these questions or use them as a guide, adding or adjusting them to meet your needs.

A.5 Align and Manage Supplier Relationships to Manage Risk

You are the arbiter of the risk your organization faces and the residual risk in your products and services. To the extent that any of your suppliers have risk they are passing on to you, it is your responsibility to evaluate that risk and determine whether to accept it or mitigate it. Given the current focus on elections, expect that your decisions will be scrutinized by election officials, the media, researchers, Congress, and the public.

Part of managing risk is deciding what type of relationship to have with any given supplier. Generally, you will think of your suppliers in one of two types of relationships, though there is a gradient between them: arms-length and closely-aligned. These relationships are about the supplier, not the product:

A.5.1 Arm's-Length Relationships

Arm's-length relationships have lower levels of integration. You are unlikely to know much about their practices aside from what is publicly available or what they share in a basic agreement. These types of relationships work well under one or more of three conditions:

1. The supplied item is less critical to your product
2. The supplied item is easily testable
3. The supplier is large and supplies the same product widely, including to non-election organizations

A.5.2 Closely Aligned Relationships

Closely aligned relationships are more tightly integrated. They often involve site visits, lengthy discussions, and product customization. You may be an important buyer to them and they may be an important supplier to you. Both parties spend time managing the relationship. To make these relationships work from a security perspective, you should:

1. Work to establish terms that ensure they manage risk in the same manner you do
2. Establish contract terms that provide confidence through verifiability

3 Involve them in understanding your risk, the importance of the product you are delivering, and the extent to which your products' security depends on their security

There are permutations of relationships other than the two above. One example is when the supplier is easily substitutable. In this case, you may not spend as much time developing the relationship but will want to push strong contract terms to meet your needs. Another is when the supplier needs access to your systems. Here, you need to have more careful management of their personnel to ensure that they only have access to the data they need; you also need to have a deeper understanding of their internal security posture.

With this frame of mind, you can develop a set of criteria for what an approved supplier looks like for any given aspect of your supply chain. Doing this comprehensively can be a time-intensive and complex task, but the results are meaningful reductions in risk.

A.6 Conduct Ongoing Monitoring

As with any other risk management program, there needs to be an ongoing effort to maintain an acceptable level of risk. Depending on the supplier and its criticality to you, this could mean continued testing of all products or random samples, site visits including process and product inspections, reconfirming security considerations through questionnaires, or, if you maintain an ongoing dialogue with them, regularly asking for any updates or changes that could impact you. Even if you have less formal methods in place, you should reassess significant suppliers at least annually.

Additionally, the dependencies and assumptions identified by your supply chain risk assessment can provide you with the list of items that you can push to the supplier through contract requirements or to inform your own active management. An example of pushing risk management activities to the supplier include contract requirements for service level agreements for patching newly discovered vulnerabilities.

Active management can include items such as requiring hardware and software bills of materials that allow you to assess the libraries and tools used in their development process. Bills of materials list all components in a product and are a well-established aspect of supply chain risk management. In conjunction with a monitoring program for bugs or flaws in software—such as that provided by the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®)—you can conduct management of the products directly, rather than relying on self-reporting.

Additionally, you can require independent assessments of delivered systems or services. This can include analysis, testing, and inspections of units delivered and go beyond basic monitoring. It can be especially important for critical components or for suppliers that are unable to provide sufficient evidence to make you fully confident in their practices.

Appendix B: Questions for Your Suppliers

Use this set of questions to learn more about your suppliers. Tailor them as necessary to get the information you need to meet your risk mitigation goals.

Organizational

1. Who are the owners of the supplier's organization?
   - Is any share of the organization foreign-owned? If so, by whom?
2. Who are the board members of the supplier's organization and what are their affiliations?
3. Does the supplier have a department or individual specifically tasked with managing cybersecurity supply chain risk?
4. From which locations will the hardware, software, or data be manufactured, developed, or accessible?
   - What are the administrative and facility security policies at these locations?
   - How does the supplier monitor these policies?
5. Which company-wide process certifications does the supplier hold?
   - Provide documentation of adherence to these processes.
6. What is the supplier's approach to maintaining an understanding of the threat environment, its proposed risk mitigation approaches, and identification of any residual risks?

Policies and Practices

1. What are the supplier's personnel policies regarding hiring and conduct standards, including background check, citizenship, and visa requirements?
2. What are the supplier's authorization procedures for personnel with access to sensitive information and systems?
3. Does the supplier adhere to a commonly accepted framework for identifying and remediating cybersecurity risks, with particular focus on components and information that are critical for mission success and increased attention to these elements?
   - If so, which set?
   - If not, how does the supplier describe its approach to managing cybersecurity risks? Is it willing to implement a commonly accepted framework and set of controls?
4. What is the supplier's security processes to address incident handling, response, recovery, and contingency arrangements to ensure availability?

Supply Chain Practices

1 What is the supplier's supply chain risk management and selection process for its suppliers?

2 Does the supplier use open source software as part of its solutions?

- If so, how does the supplier vet it?
- How does the supplier ensure that updates and patches are applied in a timely manner?

3 How does the supplier handle ensuring the security of content originating from non-U.S. sources?

4 How does the supplier review its suppliers and their products to ensure that they do not contain security vulnerabilities or malicious content and are free from unexpected or unwanted procedures?

5 Which processes does the supplier use to monitor compliance of suppliers to requirements of their respective contracts?

- Describe any process for auditing the suppliers' ability to maintain security in their development process.

6 How will the supplier share information regarding supply chain issues with its customers?

7 What is the supplier's process for managing hardware and software that is no longer supported by the supplier to ensure continued maintenance of appropriate security?

- What is the supplier's transition process for changes in suppliers to ensure security measures are continuously met?

8 Do you rely on an outside evaluator for assessing your supply chain risk?

Appendix C: Supply Chain Guidance for Election Officials

Understanding and managing supply chains is as important for election officials as it is for election technology providers.

Similar to the guidance elsewhere in this document, election officials need to be able to:

- Identify and document their supply chain
- Assess risks and prioritize components and services based on the most significant threats
- Identify and document relationships with suppliers, and align them appropriately to manage risk
- Conduct ongoing assessment and monitoring, with particular focus on identified critical components

In addition to a formal program, election officials can learn a great deal from each other, whether through the EI-ISAC, EIS-GCC, regional CISA Cybersecurity Advisors, or informal discussions with each other. These are all important to comprehensively managing risk, whether specific information about suppliers or general information about best practices to manage supply chain risk.

Election officials should leverage CIS's *A Guide for Ensuring Security in Election Technology Procurements* to help manage all cybersecurity risks associated with election technology. Many of the best practices included in the guide overlap with supply chain risk management.

Specifically, Best Practice 23 from that guide provides a set of questions election officials should ask prospective vendors. These questions are relevant for election officials trying to ensure the technology providers they use for election equipment are taking the proper actions to mitigate supply chain risk:

Best Practice #23

Proposer's supply chain management and selection process for suppliers and managing transitions when necessary, including contractor's approach to evaluating replacement components or new technologies evaluated for use in the environment to ensure adequate security.

If open source software is part of the proposed solution, explain how you will vet the software.

Suggested RFP Language

Detail your approach to supply chain management, including the selection process for suppliers. Provide specific information including, but not limited to:

- 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.
- How is information regarding supply chain issues shared among the organization and suppliers?
- 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?
- Additionally, what is your proposed approach to evaluating replacement components or new technologies to ensure adequate security?

Characteristics of Good Responses

- Processes described provide confidence that proposer carefully evaluates origins and specific security characteristics of new technology or replacement components. Evidence of certifications or, absent certifications, evidence of supply chain risk management activities, such as requiring suppliers to follow established best practices such as NIST SP 800-161. The response should describe compliance monitoring requirements, testing practices, and (if not provided elsewhere) work locations.
- 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.

Characteristics of a Bad Response

- 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.

Additionally, review Best Practices 21 and 30 for additional relevant information, and implement as many of the practices as are applicable to the specific procurement.

Appendix D: Resources

CIS Publications

- *A Handbook for Elections Infrastructure Security*
- *A Guide for Ensuring Security in Election Technology Procurements*
- *Security Best Practices for Non-Voting Election Technology*
  All available at https://www.cisecurity.org/elections-resources/.
- CIS Controls. Available at https://www.cisecurity.org/controls/.

Relevant CISA Publications and Information

- *CISA Information and Communications Technology Supply Chain Risk Management*. Available at https://www.cisa.gov/supply-chain.
- CISA Election Security Resoruce Library. Available at https://www.cisa.gov/election-security-library.

Relevant NIST Publications

- NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.
- NIST Special Publication 800-88: Guidelines for Media Sanitization. Available at https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final.
- NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations. Available at https://csrc.nist.gov/publications/detail/sp/800-161/final.
- NIST SP 800-207: Zero Trust Architecture. Available at https://csrc.nist.gov/publications/detail/sp/800-207/final.

Other Relevant Publications and Information

- Department of Labor Office of Federal Contract Compliance Programs: Debarred Companies. Available at https://www.dol.gov/agencies/ofccp/debarred-list.
- National Agency Check Information. Available at https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

CIS Center for Internet Security®

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity