SUPPLY CHAIN RISK MANAGEMENT FOR ELECTION-RELATED SOFTWARE, HARDWARE, AND SERVICES

Working Group: Threats, Vulnerabilities, Risks and Mitigation

March 4, 2022
revised May 1, 2024 and May 27, 2026

Government Facilities Sector,
Election Infrastructure Subsector
Coordinating Council

This page intentionally left blank

EXECUTIVE SUMMARY

This document has been prepared by the Sector Coordinating Council (SCC) Supply Chain Risk Management (SCRM) Working Group (WG). When the U.S. Government designates a "sector" as "Critical Infrastructure," certain partnership groups are developed, including a Government Coordinating Council composed of government officials associated with that infrastructure and a Sector Coordinating Council (SCC) composed of industry representatives associated with that infrastructure. The SCC is a self-organized and self-governed council that enables critical infrastructure owners and operators, their trade associations, and industry representatives to interact on a wide range of sector-specific strategies. Sectors and sub-sectors of Critical Infrastructure usually have a Sector Coordinating Council and corresponding Government Coordinating Council. The SCRM WG, established by the Election Infrastructure SCC, is the United States' preeminent public-private supply chain risk management partnership, established in response to the realities of today's threats to supply chain integrity and entrusted with the critical mission of identifying and developing consensus strategies that enhance supply chain security for the elections ecosystem. The SCRM WG is a group of election industry representatives that have identified the need to provide best practices and guidance regarding the procurement of election-related software, hardware, and services.

The SCRM Working Group through this publication seeks to provide basic advice and checklists to aid election technology providers and election officials when procuring election-related software, hardware, and services in their efforts to assess and reduce risks to their election jurisdiction and supply chain partners. In today's economy, it is almost impossible not to rely on an international supply chain. As such, supply chain risk management is necessary to ensure that election officials and their supply chain partners only procure election-related software, hardware, and services from legitimate sources that have a program in place to manage supply chain integrity risks. This document

CONTENTS

1.0 WORKING GROUP TEAM MEMBERS

The EI-SCC thanks those who aided in authoring this document. These tables recognize those who contributed to either or both of the first version of the document (2022) and/or its 2024 revision. Note that organizational affiliations may have changed between then and this 2026 revision.

TABLE 1—LEADERSHIP AND ADMINISTRATIVE SUPPORT FOR SOFTWARE, HARDWARE, AND SERVICES WORKING GROUPS

Working Group Leadership	Name	Company
Co-Chairs:	Chris Wlaschin*	ES&S
	Edwin Smith*	Smartmatic
	Nimit Sawhney*	Voatz, Inc.
	Tim Hallett*	ES&S
	Kate McGregor*	Freeman, Craft, McGregor Group

TABLE 2—SOFTWARE, HARDWARE, AND SERVICES SUPPLY CHAIN WORKING GROUP MEMBERS

Name	Company
Brian Hancock	Unisyn Voting Solutions
Jim Suver**	Runbeck Election Services
Rubi Barrera	VOTEC Corporation
David Orr	Hart InterCivic
Darrick Forester	SLI Compliance
Sean McCully	VoteShield
Matt Bernhard	VotingWorks
Bruce Krochman	DFM Associates
Dan Veres	VOTEC Corporation
Jesse R Peterson	SLI Compliance
Ericka Haas**	ERIC, Inc
Lawrence Gohar	Amazon Web Services
Alan Simmons	Pro V&V
Tonya Rice	Amazon Web Services
Doug Sunde	Seachange
Steve Weingart	Freeman, Craft, McGregor Group
Raleigh Sims	Logically.ai
Jessica Myers	VotingWorks
Steele Shippey	KNOWiNK

1.1 Additional Contributors

*Samuel E. Smith, Technical Editor, Independent Scholar

** Participated in drafting more than one version of this document

The 2022 and 2024 versions were informed by communications with CISA's Election Security and Resilience Office.

2.0 BACKGROUND

In June of 2021, the Election Infrastructure Subsector Coordinating Council decided to explore establishment of an SCC Supply Chain Risk Management Working Group with the general purpose of exploring potential SCRM risks to the EI Subsector partnership. In September 2021, the SCC established SCRM Subgroups to develop SCRM risk responses for Hardware, Software, Services and Ballot Paper areas. This paper focuses on assessing and managing risks associated with the assets of Software, Hardware, and Services Supply Chains. The Working Group then reconvened in 2023 to update this document to ensure its continued accuracy and relevance in the face of evolving threats to the election supply chain. In 2026 the Executive Committee of the SCC reviewed and refreshed this document in light of changes to the elections supply chain threat model.

2.1 Purpose and Working Group Objectives

This document is an introduction to how your organization and downstream supply chain partners can better protect against supply chain risks. Its purpose is to provide the following information related to election supply chain risk management:

- Provide SCRM WG guidance on election-related supply chain risk management to assist others when procuring election-related software, hardware, and services;
- Leverage existing resources provided by the Cybersecurity & Infrastructure Security Agency (CISA) and the Information and Communications Technology (ICT) SCRM Task Force;
- Provide checklists and other resources that technology providers and election officials may use to assess their election supply chain risk management strategy;
- Identify best practices regarding election-related supply chain risk management within the election community; and
- Share resources through the election community to increase awareness of supply chain risk management practices.

2.2 Relevant Definitions

Access Control: The process of granting or denying specific requests to 1) obtain and use information and related information process services and 2) enter specific physical facilities

Commercial-off-the-Shelf (COTS): Hardware or software components that are widely available for purchase and can be integrated into special-purpose systems

Election Official: Any person who is involved with administering or conducting an election, including government personnel and temporary election workers. This may include any county clerk and recorder, election judge, member of a canvassing board, central election official, election day worker, member of a board of county commissioners, member or secretary of a board of directors authorized to conduct public elections, representative of a governing body, or other person engaged in the performance of election duties as required by the election code.

Election System/Election Technology: A technology-based system that is used to collect, process, and store data related to elections and election administration. In addition to voter registration systems and public election websites, election systems include voting systems, vote tabulation systems, electronic poll books, election results reporting systems, and auditing devices. An entire array of procedures, people, resources, equipment, and locations

associated with conducting elections.

Firmware: A specific class of software encoded directly into a hardware device that controls its defined functions and provides low-level control for the device's specific hardware (such as the firmware that initially boots an operating system)

Hardware: The physical, tangible, mechanical or electromechanical components of a system.

Information Security (IS): Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide integrity, confidentiality, and availability.

Malware (Malicious Code): Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system, for example a virus, worm, Trojan Horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malware.

Multi-Factor Authentication: Authentication mechanism requiring two or more of the following: something you know (password); something you have (token); or something you are (biometric authentication).

Open Source: Computer software with its source code (human readable code) made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone for any purpose. Open-source software may be developed in a collaborative public manner, be reviewed by multiple professional and amateur programmers, require a fee and be licensed like other software, be fully open source, or have only a portion of the software open source.

Risk Assessment: The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and safeguards that would mitigate this impact.

Security Controls: Management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

2.3 Document Structure

This document is divided into three parts: software, hardware, and services. There is a companion infographic that you should reference if your organization procures ballots, envelopes, voter guides, or similar products as it includes specific guidance regarding the paper supply chain.

3.0 SCRM FOR ELECTION-RELATED SOFTWARE

3.1 Overview

Software is integral to the functioning of the election ecosystem. Even when hand-marked and hand-counted paper ballots are used to cast votes, the election jurisdiction is tied to its software for office functions such as email, and for election-specific functions such as ballot layout and results publication. Entities wishing to attack the elections ecosystem may choose to manipulate the software used by election technology providers, election jurisdictions, and service providers to the election ecosystem.

Below is a check list of questions which may be used by election software developers, technology providers, and election officials when identifying where and from whom to obtain election software. The questionnaire contains best practices on election software supply chain risk management and may be used as a guide when vetting third party suppliers. The questionnaire includes key software principles, addresses supply chain risks, and information that technology providers and their customers should seek when determining whether to utilize a third-party supplier.

3.2 Survey

1. Does your organization develop (or integrate) custom software offerings?

    - □ Yes
    - □ No
    - □ Other: _____

    1.1 List the custom software offering(s) provided by your organization.

2. Do you implement formal organizational roles and governance responsibilities for the implementation and oversight of secure software development across the development or manufacturing process for product offerings?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

    2.1 If yes, how are roles, responsibilities, and practices validated?

3. Describe what security control framework (industry or customized) is used to define your product's security capabilities? (If none, indicate N/A)

4. Does your organization document and communicate security control requirements for your software offering?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

4.1 How are security requirements validated as part of the product development or manufacturing process?

5. How does your organization implement development and manufacturing automation to enforce lifecycle processes and practices?

6. Does your organization protect all forms of code from unauthorized access and tampering, including patch updates?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

6.1 How does your organization prevent unauthorized changes to code, both inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software?

7. Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

9. Does your organization manage the integrity of IP for its product offering?

   - □ Yes
   - □ No
   - □ Other: _____
   - □ N/A

   9.1 How does the organization archive assets associated with product development or manufacturing processes?

10. Does your organization define, follow, and validate secure coding and manufacturing practices to mitigate security risks?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

    10.1 How does your organization conduct threat modeling to determine product security requirements?

    10.2 How does your organization determine how identified risks are mitigated in product design?

    10.3 How does your organization justify risk-based decisions to relax or waive security requirements or controls?

    10.4 How does your organization validate that the offering will meet the security requirements and satisfactorily address the identified threat assessments?

11. Does your organization verify that third-party software and software libraries (including free and open-source software) provides required security requirements and controls?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

    11.1 How does your organization reduce the risk associated with using acquired software modules and services, which are potential sources of additional vulnerabilities?

12. Does your organization reuse existing, well-secured software and hardware components, when feasible, instead of duplicating functionality?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

13. Does your organization configure the compilation and build processes to improve executable security?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

    13.1 How does your organization decrease the number of security vulnerabilities in the software and reduce costs by eliminating vulnerabilities before testing occurs?

14. Does your organization implement formal vulnerability and weakness analysis practices?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

    14.1 Does your organization automate the identification of security vulnerabilities and weaknesses?

14.2 Does your organization test executable code or components to identify vulnerabilities and verify compliance with security requirements?

15. Does your organization configure products to implement secure settings by default?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

15.1 Do your organization's test offerings use hardened runtime environments?

16. Does your organization use static or dynamic code evaluation or software composition analysis tools?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

16.1 If yes, which tools and to what standards do they test?

17. Has your organization taken any steps to evaluate today's risks posed to its products due to exploits similar to the log4j vulnerability, software supply chain attacks similar to SolarWinds Orion from years past, or attacks on user authentication that allow improper system access? What about steps to respond to future COTS vulnerabilities discovered by researchers or attackers?

- □ Yes
- □ No
- □ Other: _____
- □ N/A

17.1 If yes, what steps have been taken?

17.2 What about steps taken arising from AI related threats to the security of software and the rapid ability to engineer new exploits?

18. Do your organization and key supplier organization(s) use Multi-Factor Authentication for access to code repositories?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ NA

18.1 For access to common office functions such as email?

    - □ Yes
    - □ No
    - □ Other: _____
    - □ N/A

4.0 SCRM FOR ELECTION-RELATED HARDWARE

4.1 Overview

This section document focuses specifically on supply chain risk management associated with election hardware, including purpose-built products, commercial off the shelf products (COTS), and the components contained within the aforementioned. Threats to the election hardware supply chain can include, but are not limited to, email spoofing and phishing campaigns, insider threats, physical security breakdowns, online narratives that encourage action against hardware suppliers, black or gray market devices, as well as other targeted supply chain threats.

Below is a checklist which may be used by election technology providers, as well as election officials, when identifying where and from whom to obtain election hardware. The checklist contains best practices on election hardware supply chain risk management and may be used as a guide when vetting third-party suppliers. The checklist includes supply chain principles, key supply chain risks, and questions that election technology providers and their customers should ask when determining whether to utilize a third-party supplier. The use of this survey is two-fold: to assess your own organization and to assess and manage your supply chain partners (and their downstream supply partners).

Although these checklists provide a useful tool for election technology providers and election officials on best practices in election hardware supply chain risk management, additional resources links are shown at the end of this document.

4.2 Framework

People

Identify who within the organization shall be responsible for supply chain management. This may span multiple departments within the organization.

Policies and Procedures

Develop a supply chain management document which sets forth the policies and procedures that address security, integrity, availability, and quality of the products to be procured and the requirements for suppliers in which such products shall be procured from. This document should also include an incident response plan in the event the supply chain is compromised. The incident response plan should include procedures, roles, and responses in the event the supply chain is compromised. These must be based on industry standards and best practices.

Identify Products/Components

Identify the list of products and components which must be procured to run the business and successfully conduct elections.

Require suppliers to provide machine-readable SBOMs and HBOMs for all election hardware. This allows for automated vulnerability scanning of nested components (e.g., a specific microchip or an open-source library) as soon as new threats are discovered

Identify Suppliers

Identify the suppliers the organization will use to procure products and components. Such suppliers must meet the criteria developed under the policies and procedures document created above. Contracts must be executed with all suppliers and such contracts shall set forth the obligations of the supplier with respect to supply chain management.

Monitor and Collaborate with Suppliers

Perform risk assessments on the organization's suppliers, as well as those organizations that provide products and components to the suppliers. These may include, but are not limited to, conducting site visits, audits, inspection of products, chain of custody controls, security gap, and vulnerability analysis. Continually collaborate with the organization's

suppliers in order to mitigate supply chain vulnerabilities that may exist as well as to ensure proper security safeguards remain in place.

Diversify Suppliers

To the extent possible, identify and engage multiple suppliers to ensure the availability of products and components. All suppliers must meet the supply chain management requirements developed by the organization.

Purchase Methods/Terms

Identify and agree to the purchase methods and terms prior to any procurement. Ensure both parties agree on the payment and shipping terms.

Continual Evaluation

Continually evaluate your supply chain management document's policies and procedures. This evaluation should also include a threat analysis in order to identify areas of potential vulnerabilities as well as mitigations to such potential vulnerabilities. This shall be completed, at a minimum, annually to ensure all information is up to date and in compliance with the latest industry standard and best practices.

Purchase Methods/Terms

Identify and agree to the purchase methods and terms prior to any procurement. Ensure both parties agree on the payment and shipping terms.

Continual Evaluation

Continually evaluate your supply chain management document's policies and procedures. This evaluation should also include a threat analysis in order to identify areas of potential vulnerabilities as well as mitigations to such potential vulnerabilities. This shall be completed, at a minimum, annually to ensure all information is up to date and in compliance with the latest industry standard and best practices.

4.2.1 Framework Analysis

Both 'Identify Products/Components' and 'Identify Suppliers' speak to the adage that you cannot secure what has not been identified. Just as departments responsible for network security start by enumerating the devices on their network, supply chain security starts after identifying people, policies, and procedures, and enumerating who and what comprises your supply chain. Classifications of entities likely to be involved in your hardware supply chain include:

- Design: Malicious actors can compromise an entity designing components or circuit boards to introduce malware or unintended devices hiding in the product and may seem innocuous.
- Development and Production: Like the design stage, unwanted software, firmware, or components could be introduced during production. Firmware could be exfiltrated and modified, then replaced in the production line—now with undesirable capabilities. The factory could inadvertently acquire components that are counterfeit, gray market, improperly recycled/re-labeled/re-sold and place them into your products.
- Distribution: While in transit from the factory to your customer, malicious actors could gain access to your products and modify them.
- Maintenance: A new set of entities might gain access to your products during maintenance, while in your facility or in your customer facilities. This access can occur via a network or

physical access. Malware embedded in maintenance and upkeep software such as anti-virus also falls into this category.

- Disposal: Lack of consideration regarding how to securely dispose of faulty or end-of-life products can lead to malicious actors obtaining your products to sell via unauthorized channels or to examine your products for security exploits. Storage devices such as hard drives may contain sensitive company information that would be valuable to criminals and thus require special disposal procedures.

4.3 Checklist

4.3.1 Processes and Documentation

- ☐ What documentation and/or procedures do you follow regarding supply chain risk assessment and management? Do you require suppliers to also follow documented procedures? Provide copies of your policies, procedures, checklists including any Business Continuity Plan.
- ☐ How do you prevent counterfeit components from entering your supply chain?
- ☐ Do your Bill of Material documents call out components that have special security concerns, such as those that bear firmware? Safety concerns? Customization or other strictly supply chain concerns? Are there procedures for mitigating these special concerns?
- ☐ Do you and your key suppliers have a hardware vulnerability surveillance and management program?
- ☐ Are goods adequately protected in Finished Goods or similar areas, shipping docks, and in transit? How are raw goods handled upon receipt at your facility?
- ☐ Does supplier diversity influence sourcing decisions? If so, how/when is the criteria applied?
- ☐ Are you certain that no supplier is banned per ITAR or NDAA Section 889?

4.3.2 People

- ☐ Do you have defined roles that are accountable for supply chain risk management/supply chain performance and continuity? If so, what are these and what authorities do they have for assessing and mitigating supply chain risk?
- ☐ Do you and your key suppliers train staff to avoid common information security threats such as phishing attacks? Does the training include product specific vulnerabilities and methods to ensure these are not exploited? Does the training include response to natural disasters as well as man-made emergent situations such as active shooter drills?
- ☐ Do you and key suppliers use multi-factor authentication for both common office functions such as email and for sensitive information such as code/drawings/list of materials?

4.3.3 Software/Firmware

- □ Does your organization maintain a program to monitor which entities possess or have access to both your network/infrastructure and/or software and firmware incorporated into your products? Do you limit access to the organization's critical assets to only those that have a specific need to access such assets?

- □ Do you audit those entities to ensure they properly manage and secure your software and firmware?

- □ If given access to your infrastructure, do you audit or monitor those entities to ensure they have adequate security controls in place to safeguard that access and the information obtained through it?

- □ If you incorporate third party libraries into your software/firmware, do you have processes in place to ensure they have a known provenance and that the author takes steps to ensure their security?

- □ Do you use hardware root of trust where feasible?

5.0 SCRM FOR ELECTION-RELATED SERVICES

5.1 Overview

This section focuses specifically on supply chain risk management associated with election services and the spectrum of providers throughout the election lifecycle. These include ballot layout, data storage and management, polling place equipment deployment, results reporting, and many other service offerings. Threats to the election services supply chain can include, but are not limited to, email spoofing and phishing campaigns, insider threats, equipment damage, online narratives that could encourage citizens to threaten election workers or infrastructure, and physical security breakdowns as well as other targeted supply chain threats.

Included is a checklist which may be used by election service providers as well as election officials when identifying where and from whom to obtain election services and/or enhance the supply chain integrity of existing suppliers. The checklist contains best practices on election services supply chain risk management and may be used as a guide when vetting third party suppliers. The checklist includes supply chain principles, key supply chain risks, and questions that election technology providers and their customers should ask when determining whether to utilize a third-party supplier.

5.2 Framework

People

Identify who within the organization shall be responsible for supply chain management. This may span multiple departments within the organization. Ensure that they are familiar with risks and mitigations.

Policies and Procedures

Develop a supply chain management document that sets forth the policies and procedures that address security, integrity, availability, and quality of the services to be procured and the requirements to be placed upon suppliers, typically based on the criticality of the service(s) provided. These requirements must be based on industry standards and best practices.

Identify Products/Components

Identify the list of products and components which must be procured to run the business and successfully conduct elections.

Identify Suppliers

Identify the suppliers the organization will use to procure services and components. Such suppliers must meet the criteria developed under the policies and procedures document created above. Contracts must be executed with all suppliers and such contracts shall set forth the obligations of the supplier with respect to supply chain management. Prepare a security questionnaire to establish vendor practices around, for example, encryption, multi-factor authentication, and endpoint protection, and require that all prospective vendors complete it. Vet the ownership chain of the supplier to avoid conflicts of interest and/or bad actors as well as the supplier's security documentation and practices.

Monitor Suppliers

Perform risk assessments on the services provided to you, the organization's suppliers, and those organizations who provide services and components to the suppliers (second tier). These may include, but are not limited to, conducting site visits, audits, inspection of services, chain of custody controls, security gap and vulnerability analysis.

Diversify Suppliers

To the extent possible, identify and engage multiple suppliers to ensure the availability of products and components. All suppliers must meet the supply chain management requirements developed by the organization.

Purchase Methods/Terms

Identify and agree to the purchase methods and terms prior to any procurement. Ensure both parties agree on the payment and shipping terms.

Continual Evaluation

Continually evaluate your supply chain management document, policies and procedures. This shall be completed, at a minimum, annually to ensure all information is up to date and in compliance with the latest industry standard and best practices. Consider training and development of your service providers as regards risk management.

Control External Access

Ensure that if suppliers have access to your network, proper security measures are in place to protect your assets.

5.2.1 Framework Analysis

Both 'Identify Products/Components' and 'Identify Suppliers' speak to the adage that you cannot secure what has not been identified. Just as departments responsible for network security start by enumerating the devices on their network, supply chain security, after establishing people and policies & procedures, starts with enumerating who and what comprises your supply chain. Classifications of entities likely to be involved in your hardware supply chain include:

- Testers: The EAC accredited laboratories, private security firms, public security firms (National Labs), Homeland Security, hacker collectives/vulnerability managers
- Ballot Layout/Delivery: Tabulation system providers and their dealers, local election service providers,
  ballot printers, voters' guide printers, moving companies, United States Postal Service
- Polling Place Equipment Supply, Preparation, Retrieval: Moving companies, logistics/storage providers, warehouse management companies, Voter Registration and ePollbook providers, GIS providers
- Staffing: Temporary agencies, in-house recruitment department
- Data Management: Cloud providers, escrow providers, data quality services, third party contact and outreach providers, social media firms, results reporting software/reporting providers
- IT Management: OEM computer manufacturers, IT equipment distributors, IT support contractors especially those related to disaster recovery/back-ups/continuity of operations
- Consulting, Legal, Auditing: Contracted project management, risk management, election audit providers

5.3 Checklist

5.3.1 Processes and Documentation

- □ What documentation and/or procedures do you follow regarding supply chain risk assessment and management? Do you require suppliers to also follow documented procedures? Provide copies of your policies, procedures, checklists including any Business Continuity Plan. If these are tested, provide results and action plans.

- □ How do you prevent impersonation of all sorts in your service providers and provisioning (when you provide services)? This includes, but is not limited to, badges, surveillance, prevention of email and website spoofing and the use of DMARC or DKIM.

- □ Where do services include a tangible delivery or storage of items associated with the service? Are those goods adequately protected in Finished Goods or similar areas, shipping docks, and in transit? How about raw goods upon receipt at your or your suppliers' facility?

- □ Does supplier diversity influence sourcing decisions? If so, how/when is the criteria applied?

- □ Are you certain that no supplier is banned per ITAR or NDAA Section 889?

5.3.2 People

- □ Do you have defined roles that are accountable for supply chain risk management/supply chain performance and continuity? If so, what are these and what authorities do they have for assessing and mitigating supply chain risk?

- □ Do you and your key suppliers train staff to avoid common information security threats such as phishing attacks? Does the training include product specific vulnerabilities and methods to ensure these are not exploited? Does the training include response to natural disasters as well as man-made emergent situations such as active shooter drills?

- □ When a services partner has access to your facility or persons embedded in your offices, have you considered the risks and taken appropriate steps to ensure information and operational security? What if a service provider employee is or becomes a rogue element?

- □ Do you and key suppliers use multi-factor authentication for both common office functions such as email and for sensitive information such as lists of materials/customer information/employee information?

5.3.2 Software/Firmware

- □ Does your organization maintain a program to monitor which entities possess or have access to both your network/infrastructure and/or software and firmware incorporated into your products and sensitive documentation such as facility maps and employee rosters?

- □ Do you audit those entities to ensure they properly manage and secure your software and firmware?

6.0 CONCLUSION

Successful elections require good partnerships from all parties, including vigilance over all parties' supply chains. As we learn and understand these threats and issues, we need to work together to overcome them. Planning, maintaining a roster of supply chain partners, risk analysis, vigilance over supply partners, and navigating extended lead times are crucial actions in this current supply chain environment. The guidance outlined in this document is intended to benefit all the respective stakeholders through the election cycle. The Election Infrastructure Subsector Coordinating Council and this Supply Chain Risk Management Working Group will continue to monitor supply chain risks and will be glad to share recommendations with Subsector partners as appropriate.

7.0 ADDITIONAL REFERENCES

Information and Communications Technology Supply Chain Risk Management (CISA)

Securing The Software Supply Chain (CISA)

The Complete Guide to Open-Source Software Supply Chain Security (FOSSA)

ICT SCRM Vendor Template (CISA)

ICT SCRM Threat Scenarios Report (CISA)

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Supply Chain Risk Management (ODNI) Many links here including one-page basic SCRM summaries
and "Baker's Dozen, 13 Elements of an Effective SCRM Program" as titles with which to start

Supply Chain Sandbox (RSAC)

Software Bill of Materials (SBOM) for Cybersecurity Guide. CISA. (2025).

Election Security Exchange. (2026). *AI in Elections: Essentials for Risk Management.*

Exabeam. (2026). *Zero Trust in 2026: Principles, Technologies & Best Practices.*

Z2Data. (2025). *22 Critical Supply Chain Risks to Watch for in 2026.*