Supply Chain Risks to Election Infrastructure

Securing the complex supply chains serving our election infrastructure is mission critical and comprehensive risk analysis is an important component of this process. Here are some key considerations, recommendations for election jurisdictions and election system providers to keep in mind as they mitigate risk and maintain a strong supply chain security posture.

MITIGATIONS FOR ALL CATEGORIES:

Product/Component Identification:
Identify the products and components which must be procured and identify any special security concerns.

Supplier Identification:
Identify suppliers and ensure such suppliers meet your supply chain management security policies and procedures.

Supplier Monitoring:
Continually perform risk assessments on your suppliers as well as those organizations who provide products and components to the suppliers.

Continual Evaluation/Improvement:
Continually evaluate your supply chain management security policies and procedures to ensure they are up to date and incorporate the latest best practices.

Increased Costs & Lead Times:
Anticipate cost increases and longer lead times based on current trends and be sure your budgets and processes allow for these.

	Hardware	Software	Services	Paper Supplies
Categories	Election systems are comprised of many hardware components that are a part of a complex, globally connected supply chain. In order to protect these critical infrastructure hardware components, it is necessary to put into place a robust hardware supply chain risk management plan.	Entities wishing to attack the election ecosystem may choose to manipulate the software used by election technology providers, election jurisdictions, and service providers to the election ecosystem.	From consultant to custodian, election organizations are likely to have a wide spectrum of service providers. Some of these may seem hidden but fall under your supply chain risk management umbrella. Take an inventory of these providers.	Identifying, assessing, preventing, and mitigating the risks associated with election-related paper supplies includes ensuring reliability of the distributed and interconnected nature of paper manufacturing and its respective service supply chains.
Key Considerations	1. Identify every touch point in your hardware supply chain, from the sourcing of raw materials through delivery to your organization. 2. Prioritize risk management resources for the hardware components that are most critical to your organization. 3. Focus hardware security defense mechanisms to limit the threat of counterfeiting, information leakage, sabotage and tampering. 4. Conduct physical inspections of the hardware components to ensure all verifiable and authentic artifacts (i.e., serial numbers, unique product IDs, etc.) produced during the manufacturing process are present. 5. If you have firmware of software embedded in your products and developed or loaded by the third party, inspect its integrity on a continuous basis.	1. Implement formal organizational roles and governance responsibilities for the implementation and oversight of secure software development across the development or manufacturing process. 2. Choose and implement a security control framework (industry or customized) to define software product offering security capabilities. 3. Protect all forms of code from unauthorized access and tampering by implementing security controls and a patch management plan for your development environment. 4. Provide a mechanism for verifying software release integrity, including patch updates. 5. Verify that third-party software (including free and open-source software) meets requirements for security and controls.	1. Some service providers may have unsupervised access to your offices, server rooms, or other places where you store sensitive information. Include regular checks and audits to ensure compliance with contractual provisions and access granted to services supply chain employees and adjust access, as needed. 2. The corporate ownership of your service providers might surprise you. When you bring on new service providers be aware of investors or ownership of your service providers to identify potential concerns. 3. Use contracts to ensure key service providers background check staff, back-up sensitive information, and build and test their business continuity plans. 4. Integrate risk-based thinking into your supply chain management. Determine which are critical suppliers and manage them accordingly.	1. Paper mills are under unprecedented demand for many types of paper products. Order lead times are very long for ballot paper. 2. Other election related raw materials are also under supply chain pressure including envelope paper, mail packet inserts, stickers, toner for on-demand printers, and many other materials needed for elections. 3. Transportation challenges such as fewer drivers, less trailer availability and higher prices are contributing to delayed delivery of paper products. 4. Labor shortages are not helping the production of raw materials as well as the labor needed for transportation and delivery of these election products. 5. Urgent, last-minute orders are at risk to be fulfilled. The supply chain shortages hamper the ability of ballot and mail providers to deliver last minute orders.
Recommendation	✓ Election jurisdictions and election providers should establish a supply chain risk management plan. CISA and SCC have recommended best practices on developing a plan which will help to address vulnerabilities and disruptions at all stages of the hardware supply chain.	✓ Election jurisdictions should take advantage of CISA and SCC recommendations to detect and prevent software vulnerabilities at all stages of development and use.	✓ Think more broadly about who the service providers are to your organization. Investigate all access that they have to your facilities and networks. Remove those that are unnecessary and vet suppliers and their personnel carefully.	✓ Plan and order early. Ballot paper, envelope, and election material supply chain fulfillment are requiring the longest order lead times in decades due to unpredictable and delayed delivery times.

This product is the result of the Election Infrastructure Subsector Coordinating Council Supply Chain Risk Management Working Group • For more information on the Election Infrastructure Subsector, visit: cisa.gov/election-security