Executive Summary

Our increasingly globalized economy provides malicious threat actors with additional opportunities to exploit information technology (IT) supply chains for state government networks and systems.

Such attacks can cause sensitive citizen data to be exfiltrated and paralyze the delivery of essential government services. While our global economy offers state governments access to innovative and cost-effective commercial IT products, the worldwide design and testing of IT components also increases the complexity of monitoring for and protecting against supply chain threats. Supply chain threats could include tampering, inserting counterfeit parts into IT systems, malicious software, and even insider threats. Recent events like the SolarWinds Orion breach, the Colonial Pipeline attack, and countless other ransomware attacks have taught us that leaders at all levels must take action to proactively and holistically address these risks. The Information Technology Industry Council (ITI) recommends that state leaders leverage industry as partners to adopt a risk-based, whole of government approach to securing state IT supply chains.
Key Takeaways

Centralized Approach: Under the leadership of Governors in coordination with state and local elected officials and technology leaders and federally-funded State Cybersecurity Coordinators, states should take inventory of their most mission-critical procurements and programs, as well as designate a key agency as the IT supply chain “champion.” This agency should have jurisdiction and oversight over implementing relevant cybersecurity practices and promote government-wide cybersecurity awareness. The agency should also have the authority to quickly remove problematic IT equipment from state government networks once a threat has been identified.

Robust Funding and Investments: The average cybersecurity breach costs states between $665,000 to $40.53 million, with a median cost varying from $60,000 to as high as $1.87 million.¹ However, 50 percent of states do not have a committed cybersecurity budget to develop measures that would mitigate or prevent the crippling effect of cyber-related attacks.² Buying insecure IT products brings along hidden costs, such as the potential cost of paying ransomware if the component is compromised in a data breach. To the greatest extent possible, states should have a line-item budget for IT modernization and cybersecurity to support robust investments in secure IT infrastructure.

Procurement Processes Structured to Incentivize Security: States should leverage the procurement process to promote effective IT supply chain risk management. One way to fulfill this goal is to instruct acquisition personnel to source only from original equipment manufacturers (OEMs) and their authorized resellers to mitigate the risks of counterfeits being plugged into state networks. State procurement officials should also elevate cybersecurity as a key evaluation factor (at greater importance than cost) when picking a winning bidder.

Call to Action:
Designate A Single Agency as the State’s IT Supply Chain Champion

- Effective state-wide IT supply chain risk management will require ample communication and coordination among state government agencies.
- ITI recommends that each state designate one single agency, preferably with expertise in procurement and/or homeland security, as its IT supply chain “champion.” This agency would play a role similar to that of the U.S. government’s Federal Acquisition Security Council (FASC), which is tasked with developing government-wide IT SCRM policy guidance.
- This agency should serve as a central hub for all IT supply chain risk information sharing, operate as a point of contact for vendors, and provide guidance on how all state agencies can secure their networks and supply chains.
- The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2021 established a State Cybersecurity Coordinator in each state, which will work to prevent and respond to cybersecurity threats. Key personnel from the champion agency should work closely with their respective State Cybersecurity Coordinator.
- The “champion” agency should also be solely tasked with evaluating any supply chain risk information held about a vendor and, if the evidence deems it necessary, ban the vendor’s equipment from the state’s network.
- Any removal or exclusion decision should be made after providing the vendor with an opportunity to mitigate any identified risk themselves. This agency should also be responsible for regularly re-assessing the risk posed by any equipment on this banned list and evaluate whether the risk can be appropriately mitigated.

¹ The Cost of Malicious Cyber Activity to the U.S. Economy, The Council of Economic Advisers, White House (February 2018).
• For a guide on how to structure this body, states should look to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161, Cyber Supply Chain Risk Management Practices for Systems and Organizations. The document recommends that organizations establish an SCRM Program Management Office (PMO), which serves as a central clearinghouse for coordination among all roles involving supply chain security (IT, legal, procurement, etc.).

Call to Action:
Take Inventory of the State’s Most Mission-Critical Procurements and Programs

• An effective supply chain risk management strategy requires the recognition that not all systems, missions, and procurements are created equal. State Chief Information Officers (CIOs) should be tasked with developing a list of the state’s most sensitive, mission-critical programs, where the impact of a breach or data exfiltration will be the highest.

• Such a list should include any agency or programs that handle citizens’ personally identifiable information (PII), such as drivers’ license numbers, Medicaid data, etc. The state CIO should impose the most stringent supply chain risk management due diligence requirements on these procurements and programs. The agency head should designate an individual with the key role and responsibility for overseeing IT supply chain risk management for the agencies handling this sensitive data.

Call to Action:
Source from Original Equipment Manufacturers (OEMs) or Their Authorized Resellers

• Inauthentic end items and components can pose a substantial risk to a state’s networks. Potential impacts of counterfeits throughout the IT supply chain range from a component not receiving necessary security patches to the component being tampered with by a malicious actor.

• States can sharply reduce the risk of inauthentic components being plugged into their networks by requiring all IT products to be sourced from either the original equipment manufacturer (OEM) or the OEM’s authorized distributors or resellers.

Call to Action:
Integrate Security into IT Acquisitions

• According to a Deloitte-NASCIO joint study, many states spend only 3-5 percent of their IT budget on cybersecurity services, with 11 states spending as little as 1 percent of their budget on cybersecurity. State procurement officials must recognize that security is an essential ingredient to all IT acquisitions and must be evaluated at the same level as cost, schedule, or performance. States must recognize that buying insecure IT products brings along hidden costs, such as the potential cost of paying ransomware if the component leads to a data breach, and risks to critical infrastructure and services to citizens.

• State procurement officials should consider using cybersecurity and supply chain risk management as a non-weighted price factor in all IT acquisitions.


ITI Promoting Innovation Worldwide www.itic.org 3
Call to Action:
Prioritize IT Modernization Funding

- Protecting state networks and infrastructure should be considered a fundamental government mission and a financial priority. The recent COVID-19 crisis illuminated the risks to state government operations posed by outdated IT infrastructure. An obvious example is New Jersey’s struggle to administer unemployment benefits at the peak of the crisis while its systems were running on 40-year-old mainframes using the outdated COBOL programming language. Reliance on legacy IT equipment creates downstream supply chain risks as well since contracting personnel will have to turn to the gray market to find necessary replacement components.

- State policymakers should allocate dedicated funding for upgrading and modernizing legacy IT systems to the greatest extent possible.

Call to Action:
Allow Vendors to Attest to Their Supply Chain Risk Management (SCRM) Maturity

- A myriad of resources is available to help organizations take action to protect their supply chains, such as NIST SP 800-161 and international standards like ISO/IEC 20243. Vendors should have the opportunity during the solicitation process to proactively attest to their SCRM maturity, either through the implementation of NIST 800-161 or international standards or by demonstrating product integrity mechanisms like cryptographic code signing. Vendors should also be able to provide independent attestation of their network security practices, such as a certificate from the Cybersecurity Maturity Model Certification (CMMC) Accreditation Body and authorization from the State Risk and Authorization Management Program (StateRAMP). State procurement officials should be highly encouraged to consider such attestations when evaluating bids.

Call to Action:
Partner With Industry to Share Risk Information

- The IT vendor community has expansive knowledge of the evolving nature of cyber threats. The community stands well-positioned to serve as a resource to state governments to further facilitate efforts in determining how to manage IT supply chain risks. This is especially crucial considering that the private sector owns and operates 85 percent of critical infrastructure in the United States, and the IT industry supplies nearly the entire cyberspace infrastructure. Companies should feel empowered to share risk information they discover (such as a vulnerability found in a supplier’s product) without fear of litigation or liability-related repercussions.

- Governors should consider establishing formal risk-sharing communications channels and holding forums with vendors on supply chain risk management practices more broadly.