Improving State and Local Governments’ Acquisition Security Management

Strengthen information sharing about potential vulnerabilities in commercial technologies

Dan Lips
EXECUTIVE SUMMARY

State and local governments are on the front lines of the national effort to protect American citizens from cybersecurity attacks. They are responsible for providing public safety and managing elections. State and local agencies hold some of our most sensitive information, including financial and health records. State and local education agencies manage the personal information belonging to more than 50 million schoolchildren and their parents. All of these vital national services face serious threats from potential cyberattacks.

But state and local governments have limited cybersecurity expertise and capacity. In January 2020, the National Governors Association (NGA) and the National Association of State Chief Information Officers (NASCIO) issued a report describing state governments' increasing responsibilities for supporting the cybersecurity needs of local government agencies, which often have few resources. State governments themselves have scarce resources for addressing cybersecurity vulnerabilities among other responsibilities, including information technology management and federal regulatory compliance.

The federal government has an opportunity and a responsibility to support state and local governments' cybersecurity postures, including by sharing information about known cybersecurity threats.

One way that the federal government can assist state and local governments is by sharing information about known or perceived cybersecurity threats and by providing guidance about information technology acquisitions management.

A review of recent federal and state information technology management policies shows that federal agencies are banning the acquisition and use of certain information technology with links to nation-states that present a cybersecurity threat to the United States. But state governments and local governments continue to purchase and use certain technologies that federal government agencies have deemed unsafe. Specifically, recent reviews warn that state and local agencies continue to use Lexmark, Lenovo, and DJI technology that federal agencies have prohibited.
This report reviews publicly available information about differences in the cybersecurity acquisition policies and practices of federal, state, and local government agencies. It presents the following recommendations to Congress and the executive branch to take immediate actions to strengthen state and local governments’ cybersecurity:

1. Congress and the federal government should improve information sharing about known or perceived cybersecurity threats, consistent with the requirements of 2018 bipartisan legislation.

2. Congress and federal agencies should prohibit federal funds being used by state and local governments to purchase technology, equipment, or services that are identified to pose a cybersecurity threat to the United States by the Federal Acquisition Security Council.

3. Congress, federal agencies and federal watchdogs should partner with state and local government agencies to assess the presence of potential cybersecurity vulnerabilities within the inventories of state and local government agencies’ current information technology systems.

4. State officials and lawmakers should recognize security risks related to commercial off-the-shelf technology and pursue reforms to align state procurement policies with security recommendations from federal agencies.

Improving information sharing about known cybersecurity threats has been a priority for the federal government over the past decade, under the leadership of the Obama and Trump administrations. Bipartisan legislation passed by Congress has created a venue and legal processes for government agencies and partner organizations to share information about cybersecurity threats and vulnerabilities. In 2021 and beyond, Congress and federal agencies should prioritize sharing information about security vulnerabilities in commercial off-the-shelf technologies with state and local government agencies and other partners. Moreover, Congress should restrict the use of federal grant funding to prohibit states, localities, and tribal and territorial government agencies from purchasing technology or other equipment that would put sensitive data at risk.
BACKGROUND ON STATE AND LOCAL GOVERNMENT CYBERSECURITY CHALLENGES

In 2020, state and local governments faced significant information technology challenges related to COVID-19—including transitioning government workers to teleworking, maintaining essential services, holding a national election, and supporting the unprecedented transition to remote or virtual learning for thousands of school districts affecting millions of children.

State and local governments faced these challenges during a period when they were already facing new and increasing cybersecurity threats. In 2019, states, local governments, schools, and hospitals experienced a dramatic increase in cyberattacks, including ransomware. By one estimate, 140 “local governments, police stations and hospitals [had] been held hostage by ransomware attacks” during the first ten months of 2019. One notable victim was the City of Baltimore, which spent an estimated $18 million on a ransomware attack and related remediation expenses. Overall, cyberattacks against state and local governments have increased by 50 percent since 2017.

State and local governments have limited resources for cybersecurity, despite these rising challenges. A 2020 report published by Deloitte and the National Association of State Chief Informa-

---

tion Officers (NASCIO) highlighted the challenges facing states:

- A majority of states spent less than 3 percent of their IT budgets on cybersecurity.
- Just 18 states include a specified line item for cybersecurity in the state budget.
- Fewer than 15 states support local government and public schools by providing training or through other collaborations.
- 42 percent of state CIOs reported inadequate cybersecurity staffing.

Nevertheless, the same survey found that state government employees responsible for information technology and cybersecurity view the likelihood of security incidents in the next year to be greater than in the past.

Not surprisingly, reviews of state governments’ cybersecurity postures have identified potential vulnerabilities and weaknesses. For example, an October 2020 review by SecurityScorecard found that 75 percent of the states and territories "showed signs of a vulnerable IT infrastructure." A recent survey of state CIOs found that just half had “documented the effectiveness of [their] cybersecurity program with metrics and testing.”

According to the National Governors Association and NASCIO, state officials were seeking to provide additional cybersecurity support to local government agencies and public schools at the beginning of 2020. However, the economic effects of the COVID-19 recession are likely to create new downward pressure on state budgets. According to estimates published by the

---


11 Ibid.


Brookings Institution and the American Enterprise Institute, state and local governments will face revenue shortfalls between $167 billion and $240 billion in FY 2021.

Fewer resources for state information technology budgets likely will delay new investments to enhance state cybersecurity capacity. States will presumably focus resources to execute mandatory responsibilities, such as administering federal programs and complying with federal regulations. The latter has been identified as an ongoing problem by state CIOs. State governments report that a significant share of resources for information technology are dedicated to complying with federal data security rules, which are unnecessarily costly and at times contradictory or overlapping.

One potentially overlooked area of state and local government cybersecurity is cybersecurity risk management during the acquisition process. State officials may not have adequate resources, expertise, and information to adequately assess and manage risks in government acquisitions, such as potential vulnerabilities in commercial off-the-shelf technologies or services. Since the federal government has prioritized supply-chain risk management for federal acquisitions, this area may present an opportunity for federal agencies to enhance state and local government cybersecurity.

**RECENT EFFORTS TO STRENGTHEN U.S. CYBERSECURITY BY ADDRESSING SUPPLY-CHAIN RISKS**

In October 2020, the Federal Acquisition Security Council (FASC) issued a strategic plan for addressing and managing security risks. The strategic plan was set in motion by the President's 2017 national cybersecurity strategy and 2018 bipartisan legislation, the SECURE Technology Act, which established the council. The new plan is the culmination of four years of renewed focus on


addressing cybersecurity threats in the supply chain and managing broader national cybersecurity risks posed by foreign adversaries.

The Trump administration’s 2017 strategy identified improving supply-chain risk management as one of its priority actions for protecting federal technology and networks. The strategy explained how this involved “addressing deficiencies in the Federal acquisition system, such as providing more streamlined authorities to exclude risky vendors, products, and services when justified. This effort will be synchronized with efforts to manage supply-chain risk in the Nation’s infrastructure.”

During the Trump administration, federal agencies and Congress took aggressive steps to identify and address known vulnerabilities. In 2017, the Department of Homeland Security directed federal agencies to identify and remove Kaspersky Lab software from federal networks, which was later codified in law. The FY 2019 National Defense Authorization Act included a similar provision to prohibit federal agencies from using technology from Huawei Technologies Company or ZTE Corporation.

The SECURE Technology Act, which required the formation of the Federal Acquisition Security Council or FASC, passed in December 2018. Under this law, the OMB director was required to name a senior official to chair a council of representatives of key agencies involved with security and acquisitions policy, including the General Services Administration and intelligence community agencies. The council was to establish policies and standards for managing supply-chain risk and sharing information about potential vulnerabilities.

In 2019, President Trump issued an executive order on securing the information and communications technology and services supply chain. The order was based on a presidential finding that “foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services,” which hold sensitive information, enable digital com-

---

merce, and support critical infrastructure, “to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people.” Further, the President explained that the use or acquisition of such technology or services owned, controlled by, or subject to the jurisdiction of a foreign adversary and that it poses catastrophic risks. (This executive order has been broadly understood to involve companies with a nexus to China or Russia.)

The order established a policymaking process for the federal government to prohibit or mitigate the acquisition of technology and services that pose such a threat, including directing the Commerce Secretary to initiate a rulemaking to execute the order.

In November 2019, the Commerce Secretary issued a proposed rulemaking for public comment, which explained how the Department planned to carry out the order on a case-by-case basis. The rulemaking provided the following summary:

> Under the proposed rule, if the Secretary makes a preliminary determination, in consultation with other Federal agencies, to prohibit or mitigate a transaction, the Secretary will provide notice to the parties engaged in the transaction. Notified parties will have an opportunity to submit a position, which may include proposed measures for mitigation, prior to any final determination issued by the Secretary. The Secretary will provide an unclassified, written final determination provided to the parties that, to the extent possible, explains how the decision is consistent with the terms of the Executive Order, and, as appropriate, a summary of the final determination will also be made publicly available.

Beyond the executive order and the Department of Commerce’s rulemaking, the administration established a new process for assessing and managing supply-chain risks in the acquisition process consistent with the bipartisan The SECURE Technology Act of 2018, the FASC issued its strategic plan in 2020, outlining its mission and objectives:

> The FASC was established to address the escalating risk to federal ICT [information and
communications technology] presented by an increasingly global and opaque supply chain infiltrated by hostile actors. The FASC’s mission is to provide leadership and coordination for supply chain risk activities critical to improving the security, reliability, and resiliency of federal ICT.²⁷

The plan listed 5 core objectives, quoted here:

1. Facilitate the creation of an effective and consistent process for identifying, assessing, and responding to ICT risk, including mitigations and recommendations for exclusion and removal of ICT sources, goods, and services that pose a risk to our nation’s supply chain.

2. Ensure all federal departments and agencies have access to best practices for their respective SCRM [supply-chain risk management] functions.

3. Facilitate the creation of an effective information sharing construct to ensure all federal departments and agencies have access to information essential to their SCRM functions.

4. Facilitate the use of shared services and common contract solutions to maximize efficiency and minimize resources needed to effectively manage the ICT supply chain across the federal enterprise.

5. Improve stakeholder engagement (e.g., non-Executive Branch Federal entities, private sector and nongovernmental organizations) to enhance partnerships to reduce supply chain risk.

The plan demonstrates the federal government’s recognition of the need to strengthen its acquisition security management, as well as to provide information to nonfederal organizations to assist their supply-chain risk management.

FEDERAL AGENCIES TAKE SPECIFIC ACTIONS TO ADDRESS KNOWN VULNERABILITIES IN COMMERCIAL OFF-THE-SHELF TECHNOLOGIES

Beyond these government-wide or national efforts, specific federal agencies have taken more direct actions to prohibit the acquisition or use of certain commercial off-the-shelf (COTS) information technology with known cybersecurity vulnerabilities. In 2019, the Department of Defense Office of Inspector General audited DOD’s management of cybersecurity risks in purchasing COTS technologies. According to an unclassified summary, the Inspector General found:

*We determined that the DoD purchased and used COTS information technology items with known cybersecurity risks. Specifically, Army and Air Force [government purchase card] holders purchased at least $32.8 million of COTS information technology items, such as Lenovo computers, Lexmark printers, and GoPro cameras, with known cybersecurity vulnerabilities in FY 2018.*

Further, the IG warned: “As a result, adversaries could exploit known cybersecurity vulnerabilities that exist in COTS items purchased by the DoD.” The report, which includes significant redactions, openly discusses examples of Congress or the intelligence community warning that a COTS technology posed a cyber and national security risk, yet Defense Department employees were still purchasing the item years later.28

A prominent example of a commercial off-the-shelf technology with reported cybersecurity vulnerabilities that federal agencies have increasingly warned about is DJI drones. In 2017, the U.S. Army banned the use of drones made by the Chinese company.29 In 2019, the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) issued a warning about DJI drones citing general concerns about technology that may allow data to be accessed

---


by Chinese intelligence services, according to CNN.\textsuperscript{30} In January 2020, the Interior Department announced that it was grounding its fleet of DJI drones.\textsuperscript{31}

The delay between the times when certain federal agencies identify cybersecurity vulnerabilities and subsequent actions to prohibit the use of vulnerable technologies highlights the policymakers' concerns about cybersecurity risk management in the supply chain and acquisitions process. This track record of delayed action to address known vulnerabilities raises questions about the timeliness and value of the federal government’s process for sharing cybersecurity threat information among federal agencies as well as its partners.

**EXAMPLES OF STATE AND LOCAL GOVERNMENT AGENCIES ACQUIRING COMMERCIAL OFF-THE-SHELF TECHNOLOGIES WITH REPORTED CYBERSECURITY VULNERABILITIES**

Recent reviews of state government and public safety agencies’ procurements show that commercial off-the-shelf technologies prohibited by federal agencies are still commonly used at the state and local level.

**LEXMARK AND LENOVO**

In 2020, Dr. Roslyn Layton, visiting fellow with the American Enterprise Institute, published a report for *China Tech Threat* detailing how state governments were purchasing technology prohibited by the Department of Defense, specifically Lexmark and Lenovo equipment.\textsuperscript{32} Layton wrote:

> A sample of publicly-available contracts negotiated between state governments and Chi-

---


inese technology vendors shows that information transmitted on the vendors’ equipment is now subject to collection, transfer, processing and inspection by the vendor, and could be transferred to any country where the vendor does business and to any entity with whom it works. For example, one US sales agreement with technology manufacturer Lenovo states that data [...] collected on devices can be transferred to any country where Lenovo does business. In any event, China’s 2017 National Intelligence Law compels this.  

Layton reviewed current state government contracts with these Chinese companies, including through contracting vehicles established by the National Association of State Procurement Officials (NASPO). Layton reported:

*NASPO negotiated contract templates for 33 states with Lenovo for computer equipment or servers. Among those 33, 10 have additional contracts with Lexmark for printers, copiers or print services. However, of the 17 states outside of the NASPO agreement, more than half also have purchased equipment directly.*

The report highlighted additional state contracts and examined contractual agreements that specify that data can be transferred outside of the country.

**DJI DRONES**

State and local governments also continue to use DJI drones, despite prohibitions and warnings by federal security agencies in recent years. In 2017, while the Department of Defense was taking steps to prohibit their use, DJI was establishing a partnership with state, local, and tribal governments to integrate drones into U.S. airspace. More than 20 states have received donated drones from DJI. By one estimate, DJI donated 100 drones to 45 police departments across 22

---

33 Ibid.

34 Ibid.

35 Ibid.


states for the purpose of COVID-19 relief.\textsuperscript{38}

A Bard College researcher compiled and analyzed data on state and local government usage of drones in 2020, finding “1,578 state and local police, sheriff, fire, and emergency services agencies in the U.S. that are believed to have acquired drones.” Nearly 90 percent of these drones were manufactured by DJI, according to data presented in his report.\textsuperscript{39}

Security researchers have identified vulnerabilities within DJI drone technology that allow data to be accessed remotely and transferred to China.\textsuperscript{40} Given Chinese law, the company would be required to provide any requested information to the government. In a 2016 interview, DJI acknowledged that it would comply with Chinese law requiring that information be transferred to the government.\textsuperscript{41} In 2020, former CISA Director Christopher Krebs told Congress that “any information collected by DJI drones should be considered at risk and protected from inadvertent disclosure.”\textsuperscript{42}

In May 2020, Republican members of the House Judiciary Committee wrote a letter to the Justice Department and DHS requesting information about security risks related to the use of DJI drones in the United States. “Although federal law enforcement agencies have warned of potential information security concerns with DJI drones,” the members wrote, “it is not clear whether state and local law agencies are fully aware of these issues.” The members asked for information about state, local, territorial, and tribal law enforcement agencies’ use of federal grant funding to purchase DJI equipment, actions taken to address security threats, and related policies and procedures.\textsuperscript{43}

These ongoing questions and the prevalence of DJI drones’ use among state and local law enforcement agencies suggest that the federal government has not adequately informed its part-
ners or the public about potential security vulnerabilities in commercial off-the-shelf hardware.

**RECOMMENDATIONS**

Given the important role that states play in managing sensitive information and supporting the protection of the nation’s critical infrastructure, including election systems, one might assume that the federal government was actively warning state governments about potential security vulnerabilities in COTS technology. Unfortunately, this is not the case.

1. **Congress and the federal government should improve information sharing about known or perceived cybersecurity threats, consistent with the requirements of 2018 bipartisan legislation.**

   The Federal Acquisition Security Council’s 2020 strategic plan highlights the need for strengthened information sharing and stakeholder engagement with nonfederal partners. Improving information sharing about cybersecurity risks and vulnerabilities has been a long-standing, bipartisan goal for federal agencies. Congress and the executive branch, including the Department of Homeland Security, should prioritize information sharing about commercial off-the-shelf technologies to nonfederal partners. For example, Congress could pass legislation requiring that the Federal Acquisition Security Council prepare an annual report to be distributed with nonfederal partners about known vulnerabilities in COTS technology.

2. **Congress and federal agencies should prohibit federal funds being used by state and local governments to purchase technology, equipment, or services that are identified to pose a cybersecurity threat to the United States by the Federal Acquisition Security Council.**

   The gap between federal and state agencies’ security practices for commercial off-the-shelf technologies with known cybersecurity vulnerabilities highlights significant inconsistencies in cybersecurity acquisitions policies and practices at the federal, state, and local levels. A troubling consequence of these inconsistencies is that federal grant funding is likely being used to help state and local authorities purchase technology and equipment that the federal government views to be unsafe. For example, the Department of Homeland Security and Department of Justice provide grants to state and local authorities. DHS has provided $54 billion to partners since
2002, including nearly $1.8 billion in FY 2020. Meanwhile, the Department of Justice awarded 2.7 billion in grants in FY 2019.

In October 2020, the Department of Justice issued an order prohibiting DOJ grant funding from being used to purchase unmanned aerial vehicles from “any entity that is determined or designated, within the Department of Justice, to be subject to or vulnerable to extrajudicial direction from a foreign government.” DOJ and DHS could enact similar policies for all commercial off-the-shelf technologies determined to pose a security threat. Moreover, Congress could enact legislation prohibiting DHS and DOJ grants from being used to purchase certain equipment based on recommendations by the Federal Acquisition Security Council.

3. Congress, federal agencies, and federal watchdogs should partner with state and local government agencies to assess the presence of potential cybersecurity vulnerabilities within the inventories of state and local government agencies’ current information technology systems.

Given states’ limited resources for cybersecurity, Congress, federal agencies, and federal watchdog organizations should provide support to help state and local governments review technology inventory to address potential vulnerabilities. For example, Congress could direct the U.S. Government Accountability Office or Inspectors General to conduct audits of state and local partner acquisitions that were made using DHS or DOJ grant funding to identify vulnerable technology that has been purchased in the past. Federal agencies, such as the Department of Homeland Security, could provide voluntary technical assistance to state and local governments to conduct security reviews of existing information technology assets.

4. State officials and lawmakers should recognize security risks related to commercial off-the-shelf technology and pursue reforms to align state procurement policies with security recommendations from federal agencies.

State officials and lawmakers need not wait for federal assistance to take actions to improve the


security of their management of technology acquisitions. For example, governors could direct state agencies to review federal agencies’ prohibitions of certain COTS technologies and take similar actions. Similarly, state legislators could pass laws to restrict state government funding from being used to purchase technology with known cybersecurity vulnerabilities.

CONCLUSION

Improving information sharing about known cybersecurity threats has been a priority for the federal government over the past decade, under the leadership of the Obama and Trump administrations. Bipartisan legislation passed by Congress has created a venue and legal processes for government agencies and partner organizations to share information about cybersecurity threats and vulnerabilities. In 2021 and beyond, Congress and federal agencies should prioritize sharing information about security vulnerabilities in commercial off-the-shelf technologies with state and local government agencies and other partners. Moreover, Congress should restrict the use of federal grant funding to prohibit states, localities, and tribal and territorial government agencies from purchasing technology or other equipment that would put sensitive data at risk.
DAN LIPS

DAN LIPS is the Director of Cyber and National Security Policy at the Lincoln Network. Prior to Lincoln, Lips served as Assistant Vice President for Policy and Government Affairs at the Internet Security Alliance. Previously, from 2011-2019, Lips worked on the staff of the U.S. Senate Homeland Security and Governmental Affairs Committee, including serving as the majority staff’s homeland security policy director. His legislative accomplishments include bipartisan legislation to modernize federal information security management and to authorize the Department of Homeland Security’s cybersecurity programs. He was the lead staff author of former Sen. Tom Coburn’s final oversight report: A Review of the Department of Homeland Security’s Missions and Performance.

Before working on Capitol Hill, Lips served as an analyst with the Federal Bureau of Investigation, focusing on cybersecurity and intelligence. From 2000 to 2010, he worked for federal and state think tanks, concentrating primarily on education policy, including serving as a senior policy analyst with the Heritage Foundation. He earned a bachelor’s in politics from Princeton University, and a master’s degree in Statecraft and National Security Affairs from the Institute of World Politics.