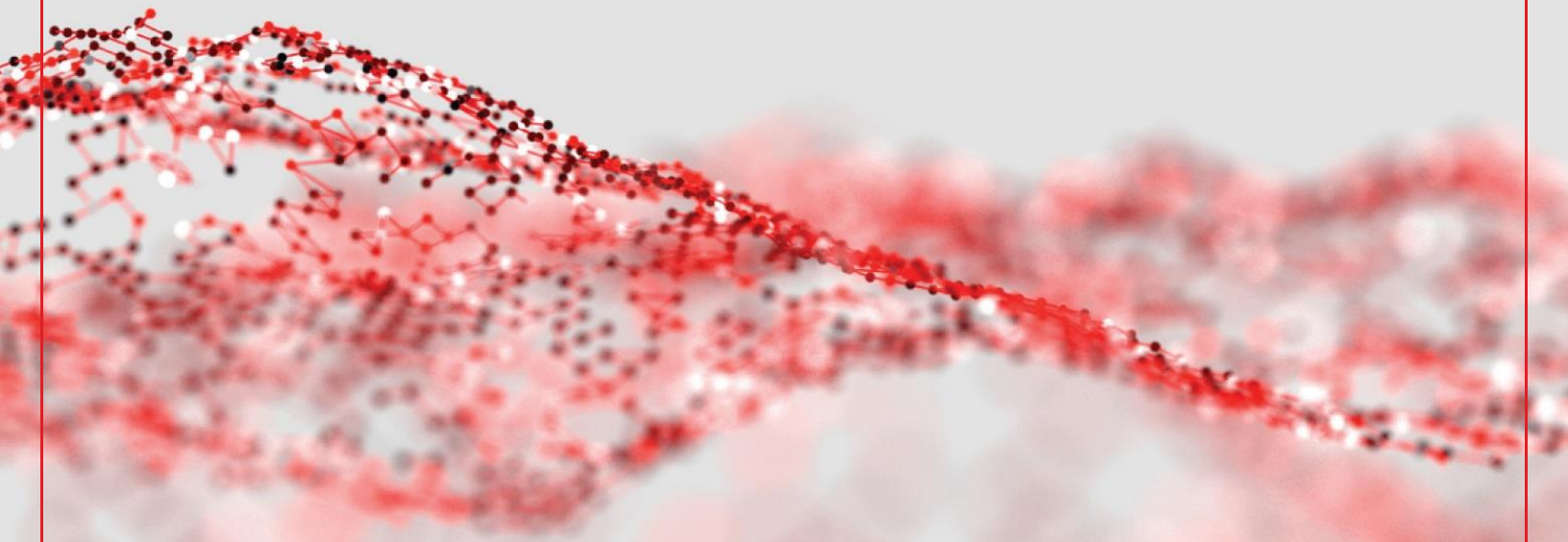
# Stealing From the States: China's Power Play in IT Contracts

## US State Governments' Failure to Scrutinize the Purchase of Lenovo and Lexmark Equipment Jeopardizes Data Security

*Updated March 2020*



China TECH THREAT

# Stealing From States: China's Power Play In IT Contracts

## State Governments' Failure to Scrutinize the Purchase of Lenovo and Lexmark Equipment Jeopardizes Data Security

### TABLE OF CONTENTS




***By:*** *Dr. Roslyn Layton, Co-Founder, China Tech Threat; Visiting Scholar, American Enterprise Institute; Visiting Researcher, PhD Fellow, Center for Communications, Media and Information Technologies, Aalborg University*


## EXECUTIVE SUMMARY:

American policymakers and media have widely covered the controversy over Chinese-owned and affiliated technology companies Huawei Technologies Company (Huawei) and ZTE Corporation (ZTE) in recent years, but other Chinese corporations present similar threats to US national security. In July 2019 the Department of Defense Inspector General highlighted some $33 million in purchases by the Pentagon of commercial off the shelf (COTS) Lexmark and Lenovo products, which have been noted on the National Vulnerability Database because of security deficiencies. Like Huawei and ZTE, Lexmark and Lenovo are Chinese-owned and banned by multiple military and intelligence agencies in the U.S. and around the globe. This paper expands on these concerns by exploring the threats present within state governments with the purchase of Lexmark and Lenovo products.

**Key findings:**

1. Chinese information technology vendors that have been banned from US military and intelligence networks still contract with state governments. Once the products from these vendors are installed, they can access sensitive personal and financial information held by courts, police departments, elections departments, education departments, children and family services, and other social service providers and agencies.

2. A sample of publicly-available contracts negotiated between state governments and Chinese 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 can collected on devices can be transferred to any country where Lenovo does business In any event, China's 2017 National Intelligence Law compels this.

3. The National Association of State Procurement Officers (NASPO) frequently negotiates contracts on behalf of its members. However, security is not a parameter of NASPO's evaluations. While federal policy directs information security for federal agencies, states must determine their own information security standards. NASPO's collective contract with Lenovo was initiated in 2015 and ends in March 2020; Lexmark's collective agreement with organization ends in 2021.



ChinaTechThreat.com
Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com

## BACKGROUND:

At the federal level, Chinese government-owned vendors Huawei and ZTE have been restricted from US federal government installations and commercial telecommunication networks because backdoors in the equipment could enable espionage, surveillance, or sabotage.[1] US states are also vulnerable to these and other Chinese vendors. Federal policy highlights that Chinese-owned technology firms present threats to national security. In addition to Huawei and ZTE, Section 889(f)(3) of the 2019 NDAA prohibits US military purchase of video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company or any subsidiary or affiliate of such entities.[2] The Department of Commerce's Entity List and National Vulnerability Database list additional Chinese controlled technology firms identified for the vulnerabilities embedded within their products.[3]

The Federal Communications Commission adopted rules that prohibit monies from Universal Service Fund, about $9 billion annually, to be used on vendors and equipment that pose a national security risk.[4] Those risks include but are not limited to surveillance, denial of service attacks, and the loss of integrity and confidentiality of networks. Huawei and ZTE are noted as covered companies in the order, and the FCC further moves to require USF recipients to remove and replace equipment from covered companies as well as to collect information to determine to what extent products and services from such covered companies exist in networks.[5]

Cyber incidents have grown exponentially more common in recent years, with the World Economic Forum listing mass data breaches and cyberattacks as two of the five largest risks facing the world in both 2018 and 2019.[6] State governments have a faced the growing trend of cyberattacks in the form of hacktivism and ransomware attacks on network infrastructure, costing governments millions of dollars and eroding public confidence in civil institutions.[7]

With state budgets increasingly stretched, low-priced Chinese technology has gained appeal. However, there is no systematic way for state procurement officers to determine whether the equipment they purchase is safe.[8] Various federal authorities review the vulnerabilities of Chinese-made information technology products, but the results of these reviews are either classified, or are not published in a user-friendly way.

Chinese hardware and software can facilitate the transfer of data to China where it can be collected, inspected, and processed by the Chinese Communist Party (CCP) and related actors.[11] While this can be done illicitly, the contracts of Lenovo and Lexmark, like other Chinese-owned firms, stipulate as much.

State government information officers rely on organizations such as NASPO to validate procurement contracts. However, information security is not currently part of NASPO's responsibility.[9] While NASPO can help a state develop a fiscally responsible procurement contract, it does not necessarily shed light of the information security of contracted products.[10] State procurement officers likely need additional tools and processes to conduct the information security assessment.

## DANGER AHEAD: CHINA'S 2017 INTERNET SECURITY LAW

In 2016 the Chinese Communist Party, through the Standing Committee of the National People's Congress, passed the China Internet Security Law which went into effect in June of 2017.[12] This law requires network operators, including all companies headquartered in China, to store select data within country and allows for Chinese authorities to do 'spot-checks' on a company's network operations.[13]

These spot checks are conducted in a way that allows for unmitigated access to information stored by "network operators and critical industry leaders." The Chinese legislation defines "network" as any system comprised of computers and related equipment that gathers, stores, transmits, exchanges or processes information – meaning the law is applicable to nearly all businesses in China that operate their own email or other data networks.[14]

Critical sectors are also defined in the law, encompassing businesses involved in communications, information services, energy transport, water, financial services, public services and electronic government services.[15] Any company that is a supplier or partner with firms in these Chinese business sectors could also be subject to the law.[16]

"… the China Internet Security Law … requires network operators, including all companies headquartered in China, to store select data within country and allows for Chinese authorities to do 'spot-checks' on a company's network operations."

Especially concerning to American business interests is Article 37 of the Chinese Intelligence Law, requiring network operators in critical sectors to store data within mainland China that is gathered or produced by any Chinese operator.[17]

Lenovo and Lexmark, Chinese controlled companies with ownership ties to the Chinese Communist Party, are subject to the aforementioned cybersecurity law, therefore posing an immense threat to Western users of these technology products. The transfer and storage of consumer data to mainland China introduces American users to the possibility of Chinese government data collection, compromising the data security and privacy of millions of Americans.

## MILITARY AND INTELLIGENCE BANS OF LENOVO AND LEXMARK PRODUCTS

In 2019, the Department of Defense Office of the Inspector General released an audit regarding the purchase of Commercial Off-the-Shelf (COTS) items by employees and the security ramifications of those purchases.[18] Referenced in that report was the purchasing of Lenovo laptops and Lexmark printers, COTS items with histories of security vulnerabilities exploitable by a technological adversary like the Chinese Communist Party (CCP).[19]

Lenovo has drawn scrutiny for its integration into defense infrastructure in the United States, as the US Air Force[20] raised concerns about Lenovo computers and the US Navy has banned the products from its platforms for more than ten years. After the installation of Lenovo servers onboard naval ships, the Navy decided to rid the defense craft of the equipment for fears of cyber-breach.[21]

Lexmark has been the subject of various reports regarding cyber threats and espionage risk, with the printer company facing allegations from various technology experts and conglomerates regarding adversarial use of the company's printers as a medium for cyber intrusion.[22] Printers, one of the least secure Internet of Things devices, store sensitive data on internal hard drives derived from the various printing jobs executed on a day-to-day basis. This sensitive data can be accessed through various software vulnerabilities in the printer, making sensitive documentation visible to adversaries and foreign actors.

## LENOVO'S CHINESE COMMUNIST PARTY CONNECTIONS AND SUSPECT PRODUCT INSECURITIES

Lenovo is the world's largest manufacturer of personal computers, growing from a two-room security guardhouse in 1984 to a global company today with headquarters in China and US headquarters in Morrisville, North Carolina.[23] What has become Lenovo today was founded in China in 1984 by Chinese computer scientist Liu Chuanzi and ten of his colleagues. The company was originally named New Technology Developer Inc., changing its name soon after founding to Legend Holdings.[24] Legend Holdings still exists today as the capital investing arm of Lenovo and is a stakeholder in other Chinese technology firms, such as Lexmark.[25]

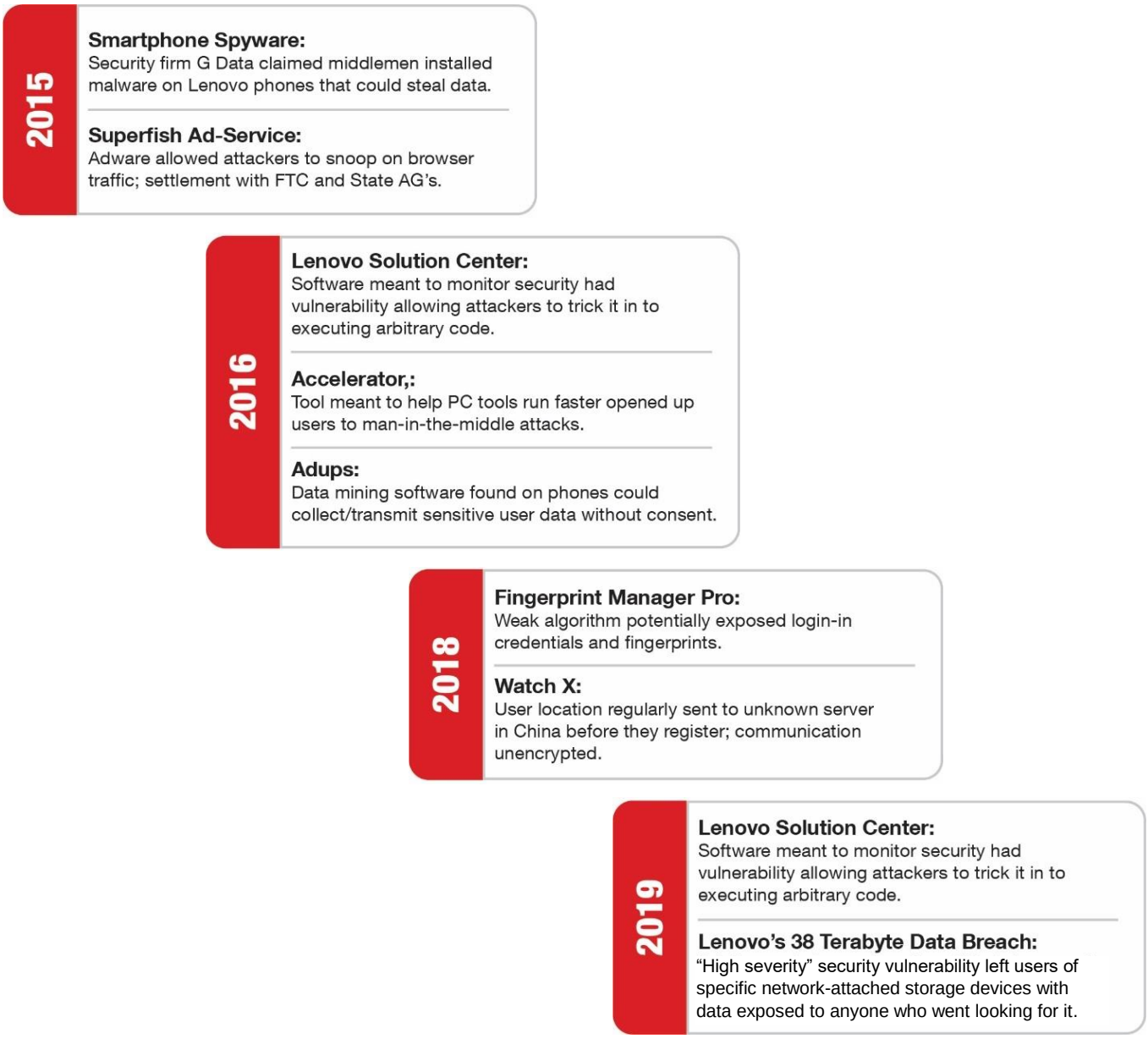
Lenovo received funding, in the amount of $25,000, from the Chinese Academy of Sciences which operates 100 research institutions in China responsive to Beijing's direction and planning. In 1984 China was very much a "planned economy," with business loans from the government rare as the state held tight control over industry and production.[26] The Chinese Academy of Sciences is considered by the USCC to be a nationally directed infrastructure of institutions, seeking to obtain technology from foreign firms in key scientific areas that often have military applications.[27] This prioritization of foreign technology acquisition can be seen directly in Lenovo's history, as the company has moved to purchase PC, server and mobile communications divisions from major American corporations.[28]

Lenovo gained position as an international computer hardware market competitor in 2005 with the company's purchase of IBM's ThinkPad division. Relatively unknown in the global marketplace before the purchase, Lenovo found itself among major players in the technology sphere, relying on the brand and name recognition of its newly acquired ThinkPad product line to compete for government contracts.[29] Shortly after the acquisition, the United States Department of State moved to purchase Lenovo laptops for employees.[32] Congressman Frank Wolf, a critic of the IBM-Lenovo deal, quickly moved to ensure the State Department understood the risks associated with using the Chinese-made machines. Congressman Wolf stated in a later interview that, "They (State Department) were not able to cancel the purchases but made sure that none of them were used for anything."[33]

The 2019 Department of Defense IG report referenced the persisting vulnerabilities present in Chinese technology, including the well-known Superfish software that was pre-installed on Lenovo laptops sold in the United States in 2014.[34] This software billed itself as a medium for advertisement targeting, but in reality served as an information aggregator to identify user trends, surveil user credentials and funnel user data to data storage centers on the Chinese mainland. Various technology news outlets referenced this bloatware as the most serious breach of user trust of the decade, with the Federal Trade Commission eventually investigating the software, fining Lenovo $3.5 million for the attempted data siphoning.[35]

In fact, Lenovo has a history of chronic and persisting vulnerabilities in their consumer products, with eight vulnerabilities documented over the past decade alone. These vulnerabilities have occurred in products ranging from personal computers to smart watches, many times compromising personal privacy and security.

At least eight such vulnerabilities have been revealed in the past five years, including:[36,37,37,39,40,41,42,43,44]



## LEXMARK'S CHINESE COMMUNIST PARTY CONNECTIONS AND SUSPECT PRODUCT INSECURITIES

While Lexmark's US operations are based in Lexington, Kentucky, the company is owned by a Chinese conglomerate including investing firms Apex, PAG Asia Capital and Legend Holdings.[45] Lexmark was acquired by the Chinese consortium in 2016 for $3.6 billion in the largest acquisition in the global printer industry.[46] Lexmark management cited the sale as a catalyst for future growth, as the company, through the new ownership, would be able to break into the lucrative Chinese market.[47]

Lexmark's connection to the Chinese government is something that has been well documents by government agencies and US courts. In a landmark case, hardware vendor Iron Bow Technologies sued the Social Security Administration (SSA) after SSA leadership concluded the Lexmark printers sold by Iron Bow posed too great a security risk to government networks.[48]

The Social Security Administration, determined to mitigate supply chain risks in procurement practices, decided that printers manufactured by Lexmark presented an unacceptable level of supply chain risk due to the company's Chinese ownership and ties to the Chinese government.[49]

In a case heard before the Court of Federal Claims, the SSA reasoned that printers connected to the agency's virtual private network (VPN) could be used to siphon sensitive data. This argument was met with stiff resistance from Iron Bow, countering the SSA's points by stating a) Lexmark printers are already in use within the Federal Government; 2) Lexmark's acquisition by the Chinese was reviewed and approved by the Federal Government under the Committee on Foreign Investment in the United States, with a requirement that a national security agreement be signed in conjunction with the purchase; and 3) that Lexmark's Chinese owners with ties to the Chinese Government were minority owners.[50]

The Court of Federal Claims ruled in favor of the SSA, stating that the CFIUS agreement with Lexmark does not address supply chain risks and that Lexmark's 49% minority ownership was enough to pose a national security risk.[51]

Lexmark has a history of software vulnerabilities in its printers, with the company cited 20 times for cybersecurity vulnerabilities by cyber research firm CVE.[87] The vulnerabilities included the storing and transmitting of sensitive network credential in plain text, absent standard encryption practices used to protect such information. The Department of Defense Inspector General stated that the vulnerabilities presented by the inclusion of Lexmark printers in government networks could allow for remote attackers to conduct cyberespionage or launch a denial of service attack on a Department of Defense Network.[88]

The Lexmark story is a case study for state and federal procurement officials. Lexmark, a company owned by Chinese financial firms, was proven in court to be corrupted by the Chinese government to the point of exclusion from the Social Security Administration's IT network.[52]

Also shown in the case of Lexmark is the danger of Chinese capital flowing into the American tech sector, as well-known brands can be purchased by foreign adversarial governments absent the knowledge of the general public. By purchasing Lexmark in 2016, Chinese investors, included those tied to the CCP and Chinese Academy of Sciences, have inserted Chinese technology into numerous sensitive government networks.

Similarly, Lexmark hardware has carried a series of security flaws in recent years, with the company's printers being the subject of multiple technical beaches.[53] The National Vulnerabilities Database lists 20 cybersecurity vulnerabilities for Lexmark, including storing and transmitting sensitive network access

credentials in plain text and allowing the execution of malicious code on the printer.[54] The 2019 DoD Inspector General Audit stated, "These vulnerabilities could allow remote attackers to use a connected Lexmark printer to conduct cyberespionage or launch a denial of service attack on a Department of Defense Network."[55]

After the release of the DoD IG Report, Lexmark released a statement saying that each Lexmark hardware issue referenced in the report had been fixed, and also called the characterization of the company in the report "unfair."[56] This response from the company does little to reconcile the security threats posed to sensitive government and private sector networks by the Chinese manufacturer.

## STATES HAVE NO STANDARD PROCESS TO EVALUATE INSECURE TECHNOLOGY

As explained above, federal policymakers in the United States have long focused on curtailing the security threats posed by Chinese-owned technology through federal regulation, neglecting the threat posed to state and local governments by malign equipment. Congress and federal agencies have given necessary attention to Chinese threats, with agencies ranging from the Department of Commerce to the United States China Economic Security Review Commission releasing recommendations and guidelines pertaining to Chinese equipment. Lost in the policy mix, however, have been state and local governments, giving Chinese manufacturers the opportunity to win massive state procurement contracts unbridled by federal government oversight.

"Certain vendors contracting with state governments through NASPO, like Lenovo and Lexmark, are banned by federal agencies – but still available for purchase by state level entities."

The leading state procurement conglomerate, the National Association of State Procurement Officers, is regarded as the "gate keeper" for state government purchasing across the United States. NASPO's ValuePoint portal notes its abilities to provide, "the highest standard of excellence in public cooperative contracting, leveraging the leadership and expertise of all states and the purchasing power of their public entities."[57] ValuePoint states that its platform provides the "highest valued, reliable and competitively sourced contracts – offering public entities outstanding prices."

Not accounted for by NASPO, or its ValuePoint procurement portal, are the security vulnerabilities existing in the products and contracts offered. By branding itself as the leading and most trusted vendor portal for state procurement officers, NASPO and ValuePoint could create a false sense of security among state officials purchasing equipment through and outside of their portals, ending in the procurement of state equipment from vendors with known and documented security vulnerabilities. By condoning the purchasing of these products, NASPO could unknowingly be increasing the volume of compromised technology purchased and used across member and non-member states. Indeed many state procurement officers, trusting the valuable work of NASPO in the past, likely assume that NASPO performs cybersecurity review even though it does not.

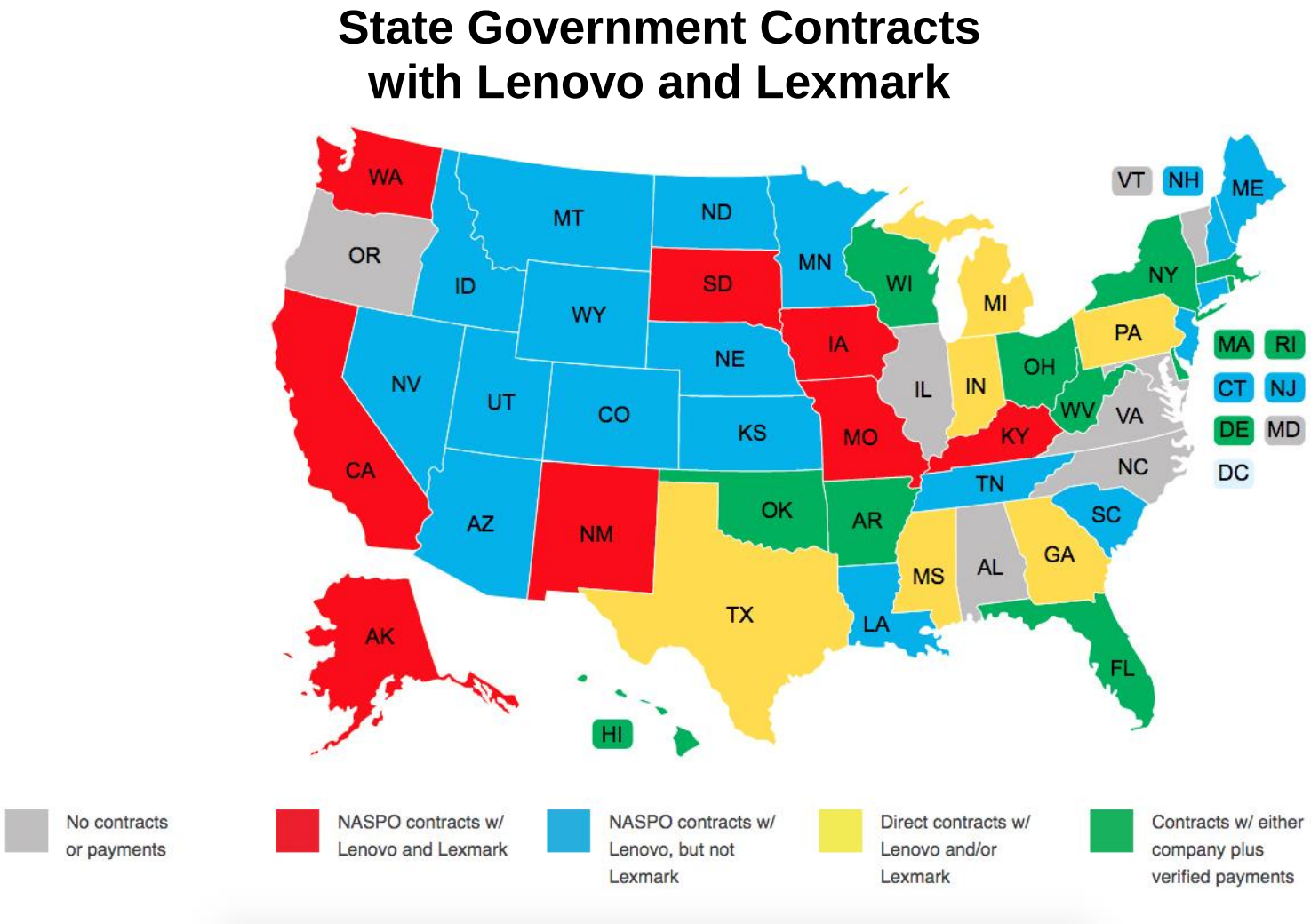
Certain vendors contracting with state governments through NASPO, like Lenovo and Lexmark, are banned by federal agencies – but still available for purchase by state level entities. This lack of continuity between state and federal officials and agencies has resulted in the widespread purchasing of compromised equipment at the state level, mostly for the sake of price, leaving citizen data at the behest of foreign actors seeking access to American data.

## EXISTING STATE CONTRACTS JEOPARDIZE SENSITIVE INFORMATION

Even while federal oversight and defense agencies warn against the use of Lenovo and Lexmark equipment in cyber networks, states governments continue to purchase from both companies. Our findings show that states purchase from Lexmark and Lenovo either through NASPO, the state purchasing conglomerate, or directly from the companies.

NASPO negotiated contract templates for 33 states with Lenovo[58] for computer equipment or servers. Among those 33, 10 have additional contracts with Lexmark for printers, copiers or print services.[59] However, of the 17 states outside of the NASPO agreement, more than half also have purchased equipment directly. Furthermore, we have verified state purchases for either company's products in a dozen states; that spending is summarized on the following pages.

| Vendor | General Description | Initial Year | Participating States |
|---|---|---|---|
| Lenovo US | Computers and equipment[60] | 2015 | 32 |
| Lenovo Global | Storage / servers[61] | 2017 | 12 |
| Lexmark | Managed print services[62] | 2019 | 5 |
| Lexmark | Copiers and managed print[63] | 2016 | 6 |



Among the state agencies contracting with Chinese controlled firms are state Supreme Courts, Departments of Health, Departments of Corrections and other law enforcement agencies, Education Departments, agencies responsible for developing IT policies and distributing IT products, and others. These state agencies are responsible for the processing and storage of some of the most private and leveragable data in the public sphere, and the introduction of malign equipment into these departments fosters unacceptable vulnerabilities .[64]

"Among the state agencies contracting with Chinese controlled firms are state Supreme Courts, Departments of Health, Departments of Corrections and other law enforcement agencies, Education Departments, agencies responsible for developing IT policies and distributing IT products, and others."

NASPO's 2015 agreement with Lenovo includes Terms and Conditions – section 7.4 titled "Customer Information" – stipulating that customer data can be transferred, stored and disclosed in any country where such action is required by law.[65]

Given the passage of China's dangerous 2017 National Intelligence Law, the terms and conditions permit the storage of data in China and the disclosure of that data to the Chinese Communist Party upon request.[66] While such a clause in contracting may be commonplace by Chinese-owned vendors, there is no reason why American data should be brought to China.

This access to citizen and government data is priceless in the hands of an adversarial government, creating a network of machines capable of delivering vast amounts of American data unabridged by court orders and legal proceedings. This access gives Chinese officials the ability to monitor and aggregate sensitive government data on American citizens – in real time.

Though the details made public about procurement and vendor payments vary among the states, available records show how Lenovo and Lexmark hardware infiltrated a myriad of state agencies, potentially exposing sensitive information of American government employees and private citizens.[67]

The next section of this paper explores case studies from Wisconsin and Arkansas, but details on several more states are readily available in Delaware, Florida, Hawaii, Massachusetts, New York, Ohio, Oklahoma, Rhode Island, Tennessee and West Virginia. Additionally, many more states hold contracts with Lexmark and/or Lenovo, but spending with the companies is unknown, including Georgia, Indiana, Michigan, Mississippi, Pennsylvania, and Texas.

**Delaware:** Since 2015, Delaware has spent over $175,000 on Lenovo equipment, with over $118,000 on computers in primary schools.[68] Other agencies spending public funds on Lenovo

hardware include the state Superior Court, state Family Court and Department of Services for Children, Youth and their Families. Since 2016, the Department of Transportation and Delaware State University spent $67,884 on Lexmark products and services.[69]

**Florida:** Since 2015, Florida agencies made over $863,000 in vendor payments to Lenovo. The agencies that spent the most on the company's services were the Department of Health ($391,885); Justice Administration ($199,684); Agency for Healthcare Administration ($121,607); Department of Corrections ($63,807); Environmental Protection ($25,686); Agency for State Technology ($23,571); and the Department of Law Enforcement ($14,198). Since 2016, the state made over $92,000 in vendor payments to Lexmark, from the Department of Highway Safety and Motor Vehicles, the State Courts System and the Department of Financial Services.[70,71]

**Hawaii:** The Hawaii Health Care Systems Corporation is authorized to spend $112,038 on Lenovo hardware and maintenance between May 1, 2019 and April 30, 2020.

**Massachusetts:** Since 2015 the Bay State has spent approximately $5 million on Lenovo products, including $4.4 million in purchases made by the Department of Transportation.[72]

**New York:** Home to the world's largest financial institutions as well as the New York Stock Exchange, the state currently possesses more than $46 million[73] in contracts with Lenovo ($2,605,000 spent) and $16 million[74] ($785,000) with Lexmark. The high-volume of Chinese equipment in state data systems presents significant risk to the data security of US and international financial markets and all New Yorkers.

**Ohio:** Last year Ohio paid[75] Lenovo $78,610. Dating back to 2015, the state spent $182,720 on Lexmark services.

**Oklahoma:** In 2019 alone, the Office of Management and Enterprise Services – the agency responsible for providing finance, property, human resources and technology services to other state offices – made $273,959 in payments to Lenovo.[76]

**Rhode Island:** Since 2015, the state has made $102,239 in vendor payments[77] to Lenovo, nearly all of money has been spent by the Office of the Public Defender ($46,259), and the Office of the Secretary of State ($46,137), the agency responsible for ensuring "elections are fair, fast and accurate."[78]

**Tennessee:** Lenovo provides laptops to state students as part of the Tennessee Department of Education's Laptop Rental Program.[79]

**West Virginia:** Beginning in 2014, West Virginia paid more than $500,000 for Lenovo products, mostly by state universities, while also spending $70,000 on Lexmark products.[80]

ChinaTechThreat.com
Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com


## CASE STUDY 1 – LENOVO IN WISCONSIN

**Background**:

The State of Wisconsin, a signee of the NASPO ValuePoint Contract MNWNC-117 (Bands 1,2,3) and MNWNC-135 (Bands 4,5) 2015-2020 Computer Equipment, Peripherals, & Related Devices, purchased $93,399.23 of Lenovo equipment in FY 2019. There were 5 departments within the state that purchased the equipment, with the largest purchase being made by the Wisconsin State Supreme Court.[81] This Chinese-manufactured equipment gives access to the Chinese Communist Party into state networks while also allowing the CCP to access that data upon request as referenced in Section 7.1 of the Lenovo User Agreement and the 2017 Chinese Cybersecurity Law.

**Risks Posed to Wisconsin State Government:**

Lenovo, the world's leading manufacturer of personal computers, is partially owned by the Chinese Academy of Sciences and compelled to comply with all Chinese cybersecurity laws as a business operating out of mainland China. Lenovo is also a market leader in the server sector, purchasing IBM's x86 server business in 2014.[82]

By procuring equipment from Lenovo, Wisconsin, state officials could be unwittingly granting access to citizen data to the Chinese government, as referenced in Section 7.4 of the 2015 Lenovo User Agreement – the same year NASPO signed a 30+ state contract with the company. This language reads:

- **7.4 Customer Information.** Lenovo and its affiliates may store, use and process contact information and other information about Customer, including names, phone numbers, addresses, and e-mail addresses, necessary to perform under this Agreement, including but not limited to warranty service. Such information will be processed and used in connection with this Agreement and the Products or Services. *It may be transferred by Lenovo to any country where Lenovo does business; and may be provided to entities acting on Lenovo's behalf in relation to this Agreement and the Products or Services. Lenovo may also disclose such information where required by law.*[83]

Buried in the later subsections of the Lenovo User Agreement, this clause gives the company permission to send user data back to China, and then disclose that data where required by law. In 2017, the Chinese government enacted a Cybersecurity Law granting access to network data from Chinese companies upon request of the Chinese Communist Party. This translates to CCP officials being able to obtain American consumer data, as Lenovo is compelled by law to share this data with party officials or risk legal reprimand from the Communist regime.[84]

**Wisconsin Agencies Procuring Lenovo Equipment in 2019 and Purchase Amounts:**[85]

- Department of Employee Trust Funds: $4,294.63
- Elections Commission: $17,431.70
- Court of Appeals: $5,872.00
- Supreme Court: $61,675.00
- Department of Revenue: $6,630.90

**Ramifications of Procurement**

With Lenovo and Lexmark's documented security vulnerabilities and a requirement to support the Chinese government, procurement officials must ask why these devices are allowed, particularly for computing responsibilities for departments of elections and courts. As the United States finds itself under attack from foreign actors, notably in its democratic elections, procurement officials should work to mitigate risk from state networks. Ridding these networks of known malign foreign equipment is a prudent step.


## CASE STUDY 2 – LEXMARK IN ARKANSAS

**Background:**

Lexmark specializes in the manufacturing of printers and printer hardware. Lexmark has a strong federal presence, with hardware in federal agencies ranging from the Department of Defense to the Internal Revenue Service. Lexmark also has a standing purchasing contract with CDW (tech equipment vendor and wholesaler) and the General Services Administration (GSA), allowing federal agencies to purchase Lexmark equipment from an online marketplace. The Lexmark privacy agreement also allows for information to be shared across national borders, namely with countries in which Lexmark operates – i.e. China, the location of Lexmark's holding companies.[86]

The Lexmark Customer Agreement for Printer and Storage Devices uses language that allows for data storage, transfer and processing in the United States and "other countries" where Lexmark maintains facilities. Given the company's operations in mainland China, Lexmark can store and process data in China and could be compelled to turn that data over the CCP.

**Lexmark Customer Agreement:**

- **Cross-border transfers:** "We are a global organization with offices and customers around the world. To efficiently manage our business and best serve you, all kinds of data – not just Personal Data – may be transferred and accessed by Lexmark entities worldwide on the basis of this Privacy Notice and in alignment with international data privacy standards. *We may store, transfer, and process Personal Data in the United States and other countries where we maintain facilities. By using our websites or services you consent to any such transfer of information outside your country."*[89]

At minimum, the language appears to violate the California Consumer Privacy Act, the new law which, failing Congressional action, is America's new de facto privacy standard.[90]

**State Focus: Arkansas**

While this paper focuses primarily on NASPO's agreements with Chinese companies, states do not need to negotiate through the organization to order Chinese-manufactured equipment. Arkansas is not a signee to the NASPO agreements with Lexmark, but has negotiated several contracts with the company since August 2018, which authorizes the state to spend $14,884,440.64; these include two separate $4.1 million contracts for "copy machines, digital" and two other $3.25 million contracts for "general equipment."[91]

Lexmark equipment and services for FY20 have already totaled more than $65,000 including the Office of Child Support Enforcement ($28,133.12), Department of Corrections ($24,321.70), and Department of Finance and Administration ($13,109.58). Given the nearly $15 million contracts in place, final spending tallies at the end of the fiscal year will likely be much higher.[92]

Besides Lexmark, Arkansas holds 36 contracts with Lenovo totaling $1,282,295. Since 2015, the state has made over $500,000 in vendor payments to Lenovo, including the Department of Health for more than $173,000 and $139,000 for the Department of Information Systems. Additional payments have been made for the Geological Survey, Administrative Office of the Courts, Supreme Court, and the Department of Education.[92]

Given the diverse missions of these agencies, their extensive reach, and how they all handle and store sensitive information, it is not a stretch to say that personal data of Arkansas residents and the data of enterprises registered in the state is at risk of being transferred to China.

**Federal Agency Purchasing of Lexmark Equipment**

Besides state agencies, the United States government contracting website, USA Spending, lists both current and past Lexmark contracts in its online database. These contracts range in transaction amount from more than $25 million to below $100,000, with agencies procuring the technology listed below.

| | | |
|---|---|---|
| *Department of Defense* | Department of the Army[93] | $453,150 |
| | Department of the Air Force[94] | $1,348,374.24 |
| *Department of Agriculture* | Chief Financial Officer[95] | $7,344,431.72 |
| *Social Security Administration* | Social Security Administration[96] | $466,369.76 |
| | Social Security Administration[97] | $25,467,857.24 |
| *Department of Transportation* | Immediate Office of the Secretary of Transportation[98] | $2,264,956.17 |
| | Federal Aviation Administration[99] | $464,337.90 |
| *National Transportation Safety Board* | NTSB[100] | $860,809.95 |
| *Department of the Treasury* | Internal Revenue Service[101] | $185,000 |

**Procurement Ramifications**

Procuring Lexmark equipment introduces systemic risk to government networks. Lexmark printers store sensitive print and network information on device hard drives and then risk exposing that information via unencrypted communication with other devices. By procuring Lexmark equipment, federal employees risk the network security of their departments while also threatening the integrity and functionality of the greater agency network infrastructure. Procurement officials should note that that denial of service attacks have been highlighted by the Department of Defense as a risk of using Lexmark equipment.[102]

## SUGGESTED REMEDIES

### #1. States Should Review Current Contracts For Security Vulnerabilities

To rid networks of persisent threats from malign Chinese technology and to ensure safety and security, states should review existing contracts with Chinese-owned vendors and assess the risks and vulnerabilities they pose. For example, what kind of liabilities would states face if sensitive data is compromised? Moreover how will state residents, businesses, and other organizations react when they learn that their valuable information can be transferred to China?

State procurement officials are gatekeepers to the data and privacy of the citizens and public entities under their purview and must understand and address the risks associated with the purchasing and use of Chinese equipment from Lenovo and Lexmark. While devices like laptops and printers seem innocuous to the average user, these network components can serve as springboards for foreign governments to spy on American citizens, collect sensitive information, and influence democratic elections. The first step in mitigating the risk associated with Chinese equipment is to take the equipment out of American networks, replacing it with trusted products. Moreover, states should reject any contract terms that allow the expropriation of data. There is no justification for data collected by US states to be shared with the Chinese government under any circumstances.

### #2. NASPO Should Consider Incorporating Cybersecurity Evaluations into its Offering or Clarify its Role

As the standard-bearer and leading state procurement conglomerate in the United States, the National Association of State Procurement Officers (NASPO) should lead the way in mitigating the threat posed to public entities procuring IT products. This begins with NASPO leaders incorporating security vulnerabilities into the contracting process. This could include partnering with federal agencies like the Department of Commerce or Department of Homeland Security's Cybersecurity & Infrastructure Security Agency (CISA) to develop for recommendations for assessing the security of products. This is especially important as NASPO renegotiates national purchasing contracts. Lenovo's state purchasing agreement with NASPO expires in March of 2020; Lexmark in 2021.

NASPO helps state procurement officials use resources wisely and improve procurement negotiation. NASPO should remind its members that cybersecurity evaluation is a separate function not included in the NASPO review. Given NASPO's experience and credibility with its members, developing competence in the information security assessment domain would add value to its members.

ChinaTechThreat.com
Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com

# Works Cited:


1. Tracy, R. (2019, November 22). FCC Deals Blow to Huawei and ZTE, Cuts Off Telecom Subsidies. Retrieved from https://www.wsj.com/articles/fcc-deals-blow-to-huwaei-and-zte-cuts-off-telecom-subsidies-11574443335
2. Thornberry, M. (2018, August 13). Text - H.R.5515 - 115th Congress (2017-2018): John S. McCain National Defense Authorization Act for Fiscal Year 2019. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/5515/text
3. U.S. Department of Commerce Adds 28 Chinese Organizations to its Entity List. (2019, October 7). Retrieved from https://www.commerce.gov/news/press-releases/2019/10/us-department-commerce-adds-28-chinese-organizations-its-entity-list
4. Tracy, R. (2019, November 22). FCC Deals Blow to Huawei and ZTE, Cuts Off Telecom Subsidies. Retrieved from https://www.wsj.com/articles/fcc-deals-blow-to-huwaei-and-zte-cuts-off-telecom-subsidies-11574443335
5. Ibid
6. Myers, J., & Whiting, K. (2019, January 16). These are the biggest risks facing our world in 2019. Retrieved from https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019/
7. Insitute, I. S. (n.d.). What Are The Biggest Security Threats To State And Local Governments? Retrieved from https://resources.infosecinstitute.com/category/enterprise/securityawareness/security-threats-by-industry/security-threats-to-state-local-governments/#gref
8. Nash-Hoff, M. (2011, August 18). Viewpoint: Why is China Cheaper? Retrieved from https://www.industryweek.com/the-economy/environment/article/21955887/viewpoint-why-is-china-cheaper
9. Who We Are. (2020). Retrieved from https://www.naspo.org/About-Us/Who-We-Are
10. Ibid
11. Lenovo Sales Agreement . (n.d.). Retrieved from https://www.lenovo.com/medias/Sales-Terms-and-Conditions-US.html?context=bWFzdGVyfHJvb3R8MTMzNzV8dGV4dC9odG1sfGg3MC9oYWMvOTQ0MTA1NTgwMTM3NC5odG1sfDgwM2RjYzkxMzNhYWYzOTJiNGEwZjU1ZjFhMWZkOGM5M2JhYzVmYTkwNzQ2OTk0ZWE5NjVkOWZiMWYwNzdhZmE
12. Creemers, R., Triolo, P., & Webster, G. (2018, June 29). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
13. Ibid
14. Ibid
15. Ibid
16. Wu, H. (2016, December 4). Final Passage of China's Cybersecurity Law. Retrieved from https://globalcompliancenews.com/final-passage-chinas-cybersecurity-law-20161204/
17. Creemers, R., Triolo, P., & Webster, G. (2018, June 29). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). Retrieved from https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/
18. Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items DODIG-2019-106. (2019, July 30). Retrieved from https://www.dodig.mil/reports.html/Article/1920236/audit-of-the-dods-management-of-the-cybersecurity-risks-for-government-purchase/?_sm_au_=iVV0tD0fjsFkZHNM01TfKK3Qv3fc4
19. Ibid
20. Gertz, B. (2016, October 24). Military Warns Lenovo Poses Cyber Spy Threat. Retrieved from https://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/
21. Muncaster, P. (2015, May 7). US Navy Looks to Dump Lenovo Servers on Security Concerns – Report. Retrieved from https://www.infosecurity-magazine.com/news/us-navy-dumps-lenovo-servers/
22. Details, C. V. E. (2019). Lexmark : Security Vulnerabilities. Retrieved from https://www.cvedetails.com/vulnerability-list.php?vendor_id=683&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=31&sha=97669f68b03c99a5cebcc8d0d0022600b1ecd781
23. Sarokin, D. (2019, February 11). The History of Lenovo. Retrieved from https://bizfluent.com/info-8081800-history-lenovo.html
24. Ibid
25. Newswire, P. R. (2016, November 29). Lexmark announces completion of acquisition by Apex Technology and PAG Asia Capital. Retrieved from https://newsroom.lexmark.com/2016-11-29-Lexmark-announces-completion-of-acquisition-by-Apex-Technology-and-PAG-Asia-Capital
26. Sarokin, D. (2019, February 11). The History of Lenovo. Retrieved from https://bizfluent.com/info-8081800-history-lenovo.html
27. Ibid
28. Holdings, L. (n.d.). Legend Holdings" Company History. Retrieved from http://www.legendholdings.com.cn/History_en/index.aspx?nodeid=1044
29. Bajarin, T. (2015, May 4). How Lenovo Became a Global PC Powerhouse After IBM Deal. Retrieved from https://time.com/3845674/lenovo-ibm/
30. Ibid
31. Ibid
32. Gross, G. (2006, May 19). U.S. State Department to limit use of Lenovo PCs. Retrieved from https://www.computerworld.com/article/2545522/u-s--state-department-to-limit-use-of-lenovo-pcs.html
33. Bartz, D. (2014, January 31). Experts predict Lenovo's U.S. buys will pass regulatory muster. Retrieved from https://www.reuters.com/article/us-motorolamobility-lenovo-regulation-idUSBREA0U06C20140131
34. Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items DODIG-2019-106. (2019, July 30). Retrieved from https://www.dodig.mil/reports.html/Article/1920236/audit-of-the-dods-management-of-the-cybersecurity-risks-for-government-purchase/?_sm_au_=iVV0tD0fjsFkZHNM01TfKK3Qv3fc4
35. Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security. (2017, December 29). Retrieved from https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled




Roslyn Layton – Roslyn@chinatechthreat.com | John Strand – John@chinatechthreat.com

36. Rubin, B. F. (2017, September 5). Lenovo settles with the feds over Superfish adware issue. Retrieved from https://www.cnet.com/news/lenovo-settles-on-superfish-adware-will-pay-3-5-million/
37. Winder, D. (2019, July 18). Lenovo Confirms 36TB Data Leak Security Vulnerability. Retrieved from https://www.forbes.com/sites/daveywinder/2019/07/17/lenovo-confirms-36tb-data-leak-security-vulnerability
38. Whittaker, Z. (2019, February 11). Lenovo Watch X was Riddled With Security Bugs, Researcher Says . Retrieved from https://techcrunch.com/2019/02/11/lenovo-watch-x-security-bugs/
39. Coppock, M. (2018, January 30). https://www.digitaltrends.com/computing/lenovo-fingerprint-manager-pro-vulnerable/?_sm_au_=iVVj67715fn2cDnc. Retrieved from https://www.digitaltrends.com/computing/lenovo-fingerprint-manager-pro-vulnerable/
40. Wiggers, K. (2017, August 1). How to keep yourself safe from Chinese spyware on budget Android phones. Retrieved from https://www.digitaltrends.com/mobile/kryptowire-adups-news/
41. Osborne, C. (2016, June 2). Lenovo begs users to uninstall Accelerator app in the name of security. Retrieved from https://www.zdnet.com/article/lenovo-begs-users-to-uninstall-accelerator-app-in-the-name-of-security/
42. George, A. (2019, August 26). Your Lenovo laptop may have a serious security flaw. Retrieved from https://www.digitaltrends.com/computing/lenovo-laptops-security-flaw/
43. Commission, F. T. (2017, December 29). Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security. Retrieved from https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled
44. Philipp, J. (2015, September 9). Spy Software Found Preinstalled on Lenovo, Huawei, and Xiaomi Smartphones. Retrieved from https://www.theepochtimes.com/spy-software-found-pre-installed-on-lenovo-huawei-and-xiaomi-smartphones_1748900.html
45. Chinese firms take over printer giant Lexmark. (2016, December 13). Retrieved from https://www.chinadaily.com.cn/business/2016-12/13/content_27658491.htm
46. Lexmark announces completion of acquisition by Apex Technology and PAG Asia Capital. (2016, November 29). Retrieved from https://newsroom.lexmark.com/2016-11-29-Lexmark-announces-completion-of-acquisition-by-Apex-Technology-and-PAG-Asia-Capital
47. Chinese firms take over printer giant Lexmark. (2016, December 13). Retrieved from https://www.chinadaily.com.cn/business/2016-12/13/content_27658491.htm
48. Federal Claims, U. S. C. of. (2018, March 27). Pre-Award Bid Protest; Judgment Upon the Administrative Record; RCFC 52.1; Supplementing the Administrative Record; Permanent Injunction. . Retrieved from https://federalnewsnetwork.com/wp-content/uploads/2018/05/ssa-supply-chain-court-case-march-2018.pdf
49. Ibid
50. Ibid
51. Miller, J. (2019, January 23). SSA bid protest win demonstrates power of acquisition to protect the supply chains. Retrieved from https://federalnewsnetwork.com/reporters-notebook-jason-miller/2018/05/ssa-bid-protest-win-demonstrates-power-of-acquisition-to-protect-the-supply-chains/
52. Ibid
53. Spring, T. (2017, December 18). User 'Gross Negligence' Leaves Hundreds of Lexmark Printers Open to Attack. Retrieved from https://threatpost.com/user-gross-negligence-leaves-hundreds-of-lexmark-printers-open-to-attack/129187/
54. Database, N. V. (2019, February 11). CVE 2019-6489 Detail. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2019-6489
55. Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items DODIG-2019-106. (2019, July 30). Retrieved from https://www.dodig.mil/reports.html/Article/1920236/audit-of-the-dods-management-of-the-cybersecurity-risks-for-government-purchase/?_sm_au_=iVV0tD0fjsFkZHNM01TfKK3Qv3fc4
56. Briefings, A. (2019, August 2). Lexmark Comments on DoD Reports Claiming Its Printers Pose Security Risk. Retrieved from https://www.action-intell.com/2019/08/02/lexmark-comments-on-dod-report-claiming-its-printers-pose-security-risk/
57. Point, N. A. S. P. O. V. (n.d.). NASPO Value Point: How It Works . Retrieved from - https://www.naspovaluepoint.org/#/page/How-it-Works
58. WELCOME TO THE LENOVO SITE FOR NATIONAL ASSOCIATION FOR STATE PROCUREMENT OFFICIALS. (n.d.). Retrieved from https://solutions.lenovo.com/naspo/
59. NASPO Managed Print Services 2016-2021. (n.d.). Retrieved February 1, 2020, from https://www.naspovaluepoint.org/portfolio/managed-print-services-2016-2021/
60. https://www.naspovaluepoint.org/portfolio/computer-equipment-peripherals-related-services-2015-2020/lenovo-united-states-inc/
61. https://www.naspovaluepoint.org/portfolio/computer-equipment-peripherals-related-services-2015-2020/lenovo-global-technology/
62. https://www.naspovaluepoint.org/portfolio/copiers-managed-print-services-2019-2024/lexmark-international-inc/
63. https://www.naspovaluepoint.org/portfolio/managed-print-services-2016-2021/lexmark-international-inc/
64. Open Book Winsconsin. (n.d.). Retrieved January 6, 2020, from http://openbook.wi.gov/PurchaseOrderDetail.aspx?AgencyCode=680&TransactionNumber=0000000296&ProviderCode=0239d537-902c-4a00-b2ad-c30c8f1a9f20&ContractId=505ENT-O16-NASPOCOMPUT-13#&&aGkjSsKEmJhEFqJgx7RzVvazW18BitPrS7n2VpJESs8iEDdGqKRy3LxuHHqL0QuvmN4Wpx dL3zkbw o ArhhO2s6cWLJ9KLlzJS7REO414IJ cfw81z2dEXWXZTb2y7F/i6p oKJYlPUFKlMzFGJw==
65. Lenovo Sales Agreement . (n.d.). Retrieved from https://www.lenovo.com/medias/Sales-Terms-and-Conditions-US.html?context=bWFzdGVyfHJvb3R8MTMzNzV8dGV4dC9odG1sfGg3MC9oYWMvOTQ0MTA1NTgwMTM3NC5odG1sfDgwM2RjYzkxMzNhYWYzOTJiNGEwZjU1ZjFhMWZkOGM5M2JhYzVmYTkwNzQ2OTk0ZWE5NjVkOWZiMWYwNzdhZmE
66. Ibid
67. Data, D. O. (n.d.). Lexmark International Broken Down by Vendor. Retrieved from https://opencheckbook.delaware.gov/#!/year/All Years/explore/0-/vendor/LEXMARK INTERNATIONAL INC/1-/department

State/Federal Contract Data:

68. https://opencheckbook.delaware.gov/?_sm_au_=iVVzrM50fpPT5ssP01TfKK3Qv3fc4#!/year/All%20Years/explore/0-/vendor/LENOVO+INC/0-/department
69. https://opencheckbook.delaware.gov/#!/year/All%20Years/explore/0-/vendor/LEXMARK+INTERNATIONAL+INC/1-/department
70. https://fs.fldfs.com/dispub2/newvpymt4.shtml

71. https://fs.fldfs.com/dispub2/newvpymt4.shtml
72. https://hands.ehawaii.gov/hands/awards/award-details/159715?_sm_au_=iVVzrM50fpPT5ssP01TfKK3Qv3fc4; http://massopenbooks.org/vendor-payments/
73. https://wwe2.osc.state.ny.us/transparency/contracts/contractsearch.cfm
74. https://wwe2.osc.state.ny.us/transparency/contracts/contractsearch.cfm
75. https://procure.ohio.gov/proc/currentContractsResults.asp?t1=0&t2=0&t3=0&CN=&IN=&SK=&CMPT=All&MT=All&KST=All%20Words&CT=ALL&CSTAT=ALL&SDT=0&SD=&ED=&CMPN=Lenovo&CTT=All%20Contract%20Types%20/%20Methods&SDTT=-%20Select%20Type%20-%20&CMPTT=&MTT=&CSTATT=All; http://ohiotreasurer.gov/Transparency/Ohios-Online-Checkbook/Advanced-Search
76. https://data.ok.gov/dataset/state-oklahoma-vendor-payments-fiscal-year-2019
77. http://www.ripay.ri.gov/VendorPayments.aspx
78. https://www.sos.ri.gov/about-us
79. https://www.tn.gov/education/district-technology/laptop-program.html
80. http://www.transparencywv.org/
81. Open Book Winsconsin. (n.d.). Retrieved January 6, 2020, from http://openbook.wi.gov/PurchaseOrderDetail.aspx?AgencyCode=680&TransactionNumber=0000000296&ProviderCode=0239d537-902c-4a00-b2ad-c30c8f1a9f20&ContractId=505ENT-O16-NASPOCOMPUT-13#&&aGkjSsKEmJhEFqJgx7RzVvazW18BitPrS7n2VpJESs8iEDdGqKRy3LxuHHqL0QuvmN4Wpx dL3zkbw o ArhhO2s6cWLJ9KLlzJS7REO414IJ cfw81z2dEXWXZTb2y7F/i6p oKJYlPUFKlMzFGJw==

Works Cited (cont.):

82. List of Lenovo's 7 Acquisitions, including Fujitsu - PC business and Marvell Semiconductor. (n.d.). Retrieved from https://www.crunchbase.com/search/acquisitions/field/organizations/num_acquisitions/lenovo
83. Lenovo Sales Agreement . (n.d.). Retrieved from https://www.lenovo.com/medias/Sales-Terms-and-Conditions-US.html?context=bWFzdGVyfHJvb3R8MTMzNzV8dGV4dC9odG1sfGg3MC9oYWMvOTQ0MTA1NTgwMTM3NC5odG1sfDgwM2RjYzkxMzNhYWYzOTJiNGEwZjU1ZjFhMWZkOGM5M2JhYzVmYTkwNzQ2OTk0ZWE5NjVkOWZiMWYwNzdhZmE
84. Ibid
85. Open Book Winsconsin. (n.d.). Retrieved January 6, 2020, from http://openbook.wi.gov/PurchaseOrderDetail.aspx?AgencyCode=680&TransactionNumber=0000000296&ProviderCode=0239d537-902c-4a00-b2ad-c30c8f1a9f20&ContractId=505ENT-O16-NASPOCOMPUT-13#&&aGkjSsKEmJhEFqJgx7RzVvazW18BitPrS7n2VpJESs8iEDdGqKRy3LxuHHqL0QuvmN4Wpx dL3zkbw o ArhhO2s6cWLJ9KLlzJS7REO414IJ cfw81z2dEXWXZTb2y7F/i6p oKJYlPUFKlMzFGJw==
86. Lexmark announces completion of acquisition by Apex Technology and PAG Asia Capital. (2016, November 29). Retrieved from https://newsroom.lexmark.com/2016-11-29-Lexmark-announces-completion-of-acquisition-by-Apex-Technology-and-PAG-Asia-Capital
87. Details, C. V. E. (2019). Lexmark : Security Vulnerabilities. Retrieved from https://www.cvedetails.com/vulnerability-list.php?vendor_id=683&product_id=0&version_id=0&page=1&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&year=0&cweid=0&order=1&trc=31&sha=97669f68b03c99a5cebcc8d0d0022600b1ecd781
88. Ward, K. (2019, August 2). Federal audit: Remote attackers could ‘use a connected Lexmark printer to conduct cyberespionage.’ Retrieved from https://www.kentucky.com/news/business/article233458527.html
89. International, L. (n.d.). Lexmark US Terms and Conditions: Privacy Notice . Retrieved from https://www.lexmark.com/en_us/privacy-policy.html
90. Becerra, X. (n.d.). California Consumer Privacy Act (CCPA). Retrieved from https://oag.ca.gov/privacy/ccpa
91. https://www.ark.org/dfa/transparency/contracts.php?ina_sec_csrf=ad9c08249a3d928802fc8b8c71c84a05&do:contracts&tab=byvendor
92. https://www.ark.org/dfa/transparency/vendor_summary.php?vendor=LENOVO+UNITED+STATES+INC
93. https://www.usaspending.gov/#/award/38399899
94. https://www.usaspending.gov/#/award/38399899
95. https://www.usaspending.gov/#/award/9276950
96. https://www.usaspending.gov/#/award/2049793
97. https://www.usaspending.gov/#/award/1647529
98. https://www.usaspending.gov/#/award/8209476
99. https://www.usaspending.gov/#/award/87385417
100. https://www.usaspending.gov/#/award/27336452
101. https://www.usaspending.gov/#/award/CONT_AWD_TIRNO09K00159_2050_GS35F0789J_4730
102. NASPO ValuePoint Lexmark Contract Information. (n.d.). Retrieved January 25, 2020, from https://www.naspovaluepoint.org/portfolio/copiers-managed-print-services-2019-2024/lexmark-international-inc/