Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology

APRIL 2018

Principal Author

Tara Beeny, Senior Business Analyst, Interos Solutions, Inc.

Subject Matter Experts

Jennifer Bisceglie, CEO, Interos Solutions, Inc.

Brent Wildasin, Managing Director, Interos Solutions, Inc.

Dean Cheng, Independent Contractor

Interos Solutions, Inc.

1725 Duke Street, Suite 510

Alexandria, VA 22314

PREPARED FOR THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Disclaimer: This research report was prepared at the request of the U.S.-China Economic and Security Review Commission to support its deliberations. Posting of the report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 113-291. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

Table of Contents

List of Tables

List of Exhibits

Acronyms

3GPP	Third Generation Partnership Project
5G	fifth generation
CAS	Chinese Academy of Sciences
CETC	China Electronics Technology Group Corporation
CNCI	Comprehensive National Cybersecurity Initiative
CNITSEC	China Information Technology Evaluation Center
CNSS	Committee on National Security Systems
COTS	commercial off-the-shelf
CSF	Cybersecurity Framework (NIST)
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DoD	Department of Defense
DRC	Democratic Republic of the Congo
FDI	foreign direct investment
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
GSA	General Services Administration
HP	Hewlett-Packard
ICT	information and communications technology
IDC	International Data Corporation
IoT	Internet of Things
IP	intellectual property
IT	information technology
ITU	International Telecommunication Union
LCD	liquid crystal display
NIST	National Institute of Standards and Technology

NIST SP	NIST Special Publication
NSA	National Security Agency
NSS	national security systems
OECD	Organisation for Economic Co-operation and Development
OEM	original equipment manufacturer
OMB	Office of Management and Budget
PLA	People’s Liberation Army
PRC	People’s Republic of China
R&D	research and development
SCRM	supply chain risk management
SD	Specialized Disclosure (SEC form)
SEC	Securities and Exchange Commission
SOE	state-owned enterprise
TRM	Technical Reference Module
VA	Department of Veterans Affairs
ZTE	Zhongxing Telecommunications Corporation

Executive Summary

The U.S. government needs a national strategy for supply chain risk management (SCRM) of commercial supply chain vulnerabilities in U.S. federal information and communications technology (ICT), including procurement linked to the People's Republic of China (China or PRC). This strategy must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on responding to vulnerabilities, breaches, and other incidents after they have already damaged U.S. national security, economic competitiveness, or the privacy of U.S. citizens.

This study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. U.S. federal government ICT supply chains are multi-tiered, webbed relationships rather than singular or linear ones. The supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the United States, including China. These products could be modified to (1) perform below expectations or fail, (2) facilitate state or corporate espionage, or (3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

Software supply chain attacks will become easier—and more prevalent—as developing technologies such as fifth generation (5G) mobile network technology and the Internet of Things (IoT) exponentially increase avenues for attack.[1] Gartner, an American information technology (IT) research and advisory firm, predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IoT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have an important impact on the ICT SCRM challenge. Relevant to this report, increasing IoT installation will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet the time required to detect those breaches is not decreasing. The responsibility of both the public and private sectors in increasing their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

China did not emerge as a key node on the global ICT supply chain by chance. The Chinese government considers the ICT sector a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. China has long-standing policies encouraging ICT manufacturing and development. These policies offer incentives for foreign companies to produce ICT in China, while at the same time pursuing opportunities to obtain key intellectual property and technology from those companies with the ultimate goal of indigenizing these technologies. Since 2013, China has accelerated its efforts at indigenous production and independence. This shift has made for a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access. At the same time, China has expanded its efforts to obtain economic advantage by pursuing knowledge of key technologies through corporate acquisitions and by using the economic power of Chinese companies as tools of the state. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain, and to U.S. national and economic security. New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and allow the Chinese government to conduct security audits on their products open federal ICT providers—and the federal ICT networks they supply—to Chinese

[1] The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

[2] Peter Middleton et al., "Forecast: Internet of Things–Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017, https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.

[3] Benoit J. Lheureux et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017, https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

cyberespionage efforts and intellectual property theft. China also continues to target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

RECOMMENDATIONS FOR A NATIONAL SCRM STRATEGY

Effective SCRM is the ability to anticipate future developments in supply chains, identity potential threats to supply chains, develop threat profiles, and mitigate or address future threats to the supply chain. Federal government laws and policies do not address SCRM comprehensively. The evolution of global production and manufacturing of ICT products and the nature of federal ICT modernization efforts means new products entering the federal information systems and national security systems have increasingly complex and globalized supply chains, many of which originate with commercial suppliers sourcing from China. It is unlikely that political or economic shifts will cause global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. How, then, should the U.S. government manage risks associated with Chinese-made products and services and the participation of Chinese companies in its ICT supply chains? Federal ICT supply chain risks can be best managed by embracing an adaptive SCRM process, centralizing the leadership of federal ICT SCRM efforts, linking federal regulations to appropriations, promoting supply chain transparency, and crafting forward-looking policies.

EMBRACE AN ADAPTIVE SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROCESS

Federal ICT modernization efforts have increased reliance on the private sector and commercial off-the-shelf (COTS) products. These new products have increasingly complex, globalized, and dynamic supply chains, many of which include commercial suppliers that source from China at multiple points within a single supply chain. These supply chains change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Nefarious actors linked to China have targeted the networks of private sector entities and private sector government contractors in order to obtain sensitive government information and to exploit vulnerabilities within federal information systems. Thus, weaknesses in the networks of industry partners pose a threat to the U.S. government and U.S. national security.

Defending against supply chain attacks by nefarious actors linked to China requires communication and collaboration with private sector actors. The National Institute of Standards and Technology (NIST) has been effective in partnering with the private sector to produce high-quality, implementable standards to improve supply chain security and cybersecurity of ICT systems, including the widely adopted NIST Cybersecurity Framework. Although NIST has been effective in these efforts, supply chain controls developed by NIST apply only to “high-impact” federal information systems.[4] Future work by NIST could include expanding supply chain standards to a broader range of federal information systems, including systems operated by private sector contractors.

Partnering with industry also means learning from experience with efforts such as the Bush-era Comprehensive National Cybersecurity Initiative (CNCI). The CNCI’s effectiveness was limited by the classified nature of its deliberations and decisions, which prevented the U.S. Department of State and the National Cyber Security Center from engaging with outside organizations, including the private sector. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere. These steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from all relevant parties.

[4] FIPS Publication 199 categorizes an information system as high impact as when “the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.” In this case, “A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.” If any of the information on a federal information system is classified as high impact with respect to confidentiality, integrity, or availability, then the entire information system is considered high impact. See National Institute of Standards and Technology, *FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, February 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

CENTRALIZE FEDERAL ICT SCRM EFFORTS

The U.S. government lacks a consistent, holistic SCRM approach. Additionally, most federal SCRM-related intelligence gathering activities are people based rather than technology based. This makes it difficult for federal SCRM programs to address the global threat comprehensively, or to scale as demand increases. The conflicting and confusing laws and regulations result in loopholes, duplication of effort, and inconsistently applied policies. Congress and the Executive Branch should encourage information sharing and the consolidation of federal SCRM leadership to optimize collection and dissemination efforts. Centralized leadership for SCRM would need to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network.[5] The Office of Management and Budget (OMB) could, through modifications to Circular A-130,[6] assign centralized SCRM authority to the General Services Administration (GSA), the U.S. Department of Homeland Security (DHS), or another federal agency. This SCRM center would provide comprehensive and authoritative data and continuous monitoring, which would reduce the need for agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations; how agencies use technology directly relates to how they apply risk mitigations. Last, such an office would need to function in the unclassified world, while at the same time having direct connections and reach-back authority into the classified environment to ensure it remains in alignment with known threats. As illustrated by the experience of the CNCI, the relationship should not be reversed and come entirely under classified control.

LINK FEDERAL REGULATIONS TO APPROPRIATIONS

Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. A near-term opportunity is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present (1) information about their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks. The current reporting is compliance oriented and does nothing to share information or increase the security posture of federal ICT networks.

PROMOTE SUPPLY CHAIN TRANSPARENCY AND PARTNERSHIP WITH INDUSTRY

Supply chain transparency increases the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government's ability to respond to, and reduce the impact of, cybersecurity incidents in an environment where supply chain attacks are ongoing. Directly in relation to the impact on national security, the federal government should promote the public listing—or at least the disclosure to the government customer—of federal ICT providers and primary or tier-one suppliers in line with actions already taken by companies such as Dell, Hewlett-Packard (HP), and Microsoft as part of their corporate responsibility efforts. The government should also push for transparency on the part of all suppliers within its own supply chain according to the level of risk management rigor required (not all programs and suppliers present the same level of risk and therefore this level of transparency may not be needed). This information does not always need to be publicly released, though audit measures should be in place to ensure the transparency exists. In taking these measures, policymakers should learn from previous supply chain transparency efforts, such as Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which required some companies to document their suppliers of "conflict minerals" in order to decrease violence in the Democratic Republic of the Congo (DRC) by limiting U.S. procurement from actors fueling conflict in the DRC. By partnering with industry and sharing information, the government customers and industry will have increased awareness of risks present in multi-tiered supplier relationships, as well as potentially effective mitigations that are already in place.

[5] A value-added reseller is a company that purchases products from a vendor (generally at a discount); adds additional features, services, or support to the existing product; and then resells the product as an "integrated" or "turn-key" solution.

[6] Circular A-130 provides policy guidance to federal agencies on the governance of IT resources, including governance, acquisitions, records management, open data, workforce, security, and privacy. The circular established minimum requirements for federal information security and privacy programs and assigns responsibilities for the security of those systems.

CRAFT FORWARD-LOOKING POLICY

Increasingly, any ICT component's physical structure pales in importance compared with the firmware and software operating within in it. Future risks will involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint research and development (R&D) efforts are also sources of risk that are not always covered in traditional SCRM. Identifying these risks and addressing them creatively as part of the adaptive approach to supply chain risk management will be important to the success of federal policy efforts.

Chapter 1: U.S. Government ICT Supply Chains

The OMB's 2017 budget proposal allocated $89.9 billion for IT in fiscal year (FY) 2017.[7] In 2016, International Data Corporation's (IDC's) Government Insights and FedScoop jointly released a study claiming that the U.S. federal ICT market is "the largest single vertical market for IT in the U.S. today, representing about 8.6 percent of all IT spending in the U.S., followed by the banking industry, at 7.6 percent."[8] FedScoop released two rankings in connection with the study: the "Top 25 Enterprise IT Providers to Government" and the "Federal IT Top 100." The top 10 companies on each list are shown in **Table 1**. Despite the size of the U.S. federal ICT market, IDC's research indicates that over 50 percent of federal IT spending goes to the top 10 suppliers on the lists, making their supply chains worthy of particular scrutiny for potential risk access points. It should be noted that Intel ranks at number 11 on the "Top 25 Enterprise IT Providers to Government" list, and also serves as a provider of primary technology components to many of the other companies in the top 10, thus its inclusion in this report.

THE FEDERAL ICT ECOSYSTEM

IDC and FedScoop's "Top 25 Enterprise IT Providers to Government" list ranks major enterprise IT companies by their estimated government-only sales.[9] The list includes the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.

The second list, the "Federal IT Top 100," ranks integrators and solution providers on the basis of revenue from the sale of IT products and services to federal agencies.[10] This list includes key players in government ICT contracting—firms that provide, manage, and, in some cases, modify the products produced by firms on the enterprise providers list.

Table 1
Federal IT Spending Ranked by Provider, FY 2015

Ranking	Top 25 Enterprise IT Providers to Government	Federal IT Top 100
1	Hewlett-Packard	Lockheed Martin
2	IBM	National Security Technologies
3	Jeppesen Sanderson (Division of Boeing)	Leidos, Inc.
4	Dell	Battelle Memorial Institute
5	Computer Sciences Corporation[1]	Northrop Grumman
6	Cisco	SAIC
7	Boeing	UChicago Argonne
8	Deloitte Consulting	Harris
9	Unisys	Consolidated Nuclear Security
10	Microsoft	Raytheon

Note: These rankings are based on actual revenues generated from the sale of IT products and services during the federal government's FY 2015, not multiyear contract awards. IDC has removed non-IT spending that is often included in IT contracts (such as management, consulting, and energy costs).

1. On April 3, 2017, Computer Sciences Corporation merged with Hewlett-Packard Enterprise Services to create DXC Technology.

Sources: IDC Government Insights and FedScoop.

[7] Phil Goldstein, "2017 Budget Boosts IT Spending to $89.9 Billion, Expands U.S. Digital Service," *FedTech*, February 9, 2016, https://fedtechmagazine.com/article/2016/02/2017-budget-boosts-it-spending-899-billion-expands-us-digital-service.

[8] Wyatt Kash, "New Top 100 Rankings Reveals Which Firms Earn the Most from Federal IT Spending," FedScoop, June 24, 2016, https://www.fedscoop.com/federal-it-top-100-report-on-government-it-spending/.

[9] "Top 25 Enterprise IT Providers to Government," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

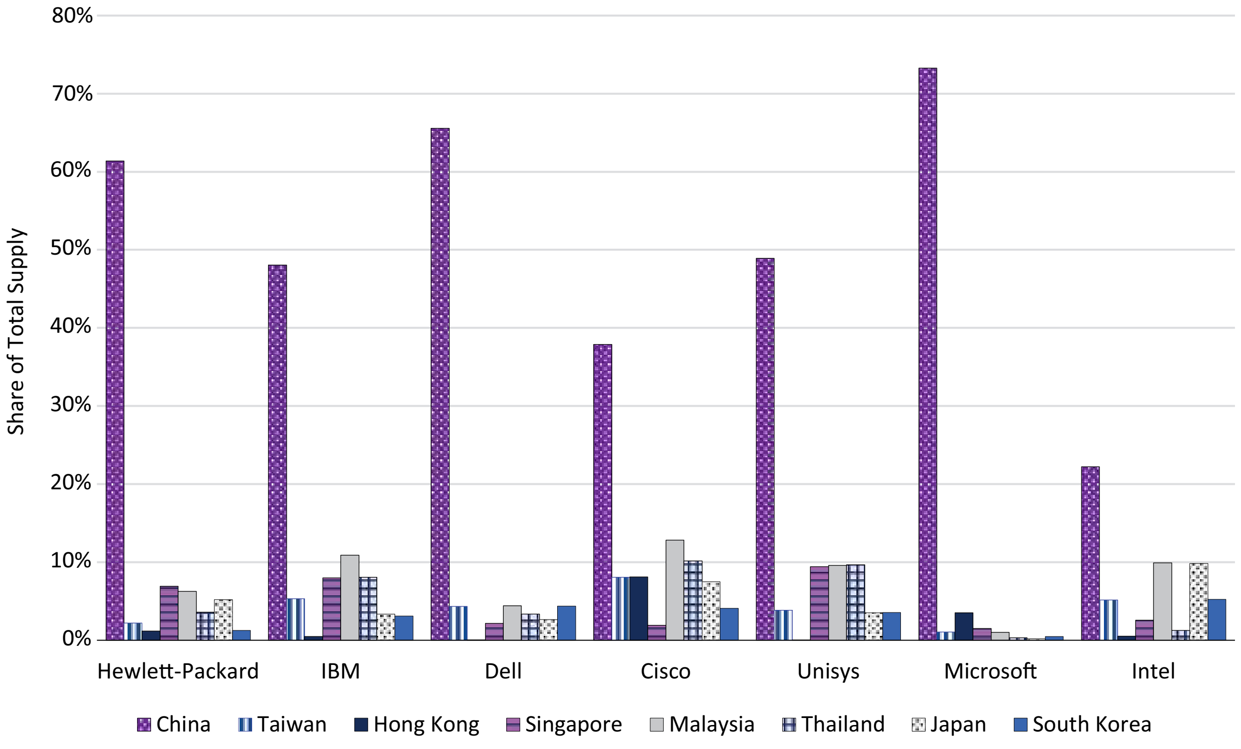
[10] "Federal IT Top 100 – Federally Focused IT Providers," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-100/full-list/.

QUANTIFYING THE CHINA SUPPLIER NEXUS

In breaking down the supply chain implications for top companies on the enterprise providers list, this report focuses on seven manufacturers: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. These seven companies are some of the top IT providers to the U.S. government that are primarily IT manufacturers, and for which sufficient open source supply chain data exist. The nature of available open source information can make it difficult to separate data from a parent company from those of its subsidiaries; for example, data for Jeppesen Sanderson are tied to data for Boeing. The available data sets for Computer Sciences Corporation and Deloitte Consulting are too small to support firm conclusions. Focusing on these seven major IT manufacturers can illustrate the trends and challenges of supply chain risk analysis for commercial IT products. This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although each company conducts some level of due diligence on its supplier base, the complete records are not publicly available. Additional analysis of the aforementioned Jeppesen Sanderson, DXC Technology, and Deloitte, as well as other top federal enterprise IT providers such as AT&T, Abacus Technology, and Amazon Web Services, would provide a more comprehensive understanding of the federal ICT ecosystem.

Exhibit 1 provides transactional data culled from publicly available information for HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. The graph shows the percentage of shipments originating in various countries between September 8, 2012, and September 7, 2017, for each company and its subsidiaries. These data provide a broader picture than U.S. trade data, as they include import and export data for other countries as well, including Bolivia, Chile, China, Colombia, Costa Rica, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela. As the chart shows, China is the overwhelming source of products for these manufacturers. An average of 51 percent of shipments to these seven commercial IT manufacturers originate in China. Microsoft has the largest share of shipments originating in China, at 73 percent.

Exhibit 1
China Supply for Seven Leading Federal IT Providers, 2012–2017



Source: Panjiva.

Over 95 percent of all commercial electronics components and IT systems supporting U.S. federal IT networks are COTS, and China's role in this global supply network is significant. The supply chain for commercial IT is a global enterprise dominated by suppliers in East Asia.[11] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) notes that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[12]

TRACING THE CHINA SUPPLIER NEXUS

Changing market dynamics and the increasing complexity of the commercial ICT supply chain have created additional challenges for supply chain risk management. During the transformation from raw materials to finished products, ICT components can transit several national borders. As one study showed, the elements that are eventually incorporated into an Apple iPod may be sourced from suppliers in the United States, Japan, Taiwan, and South Korea and assembled in plants in China run by Taiwanese corporations.[13] Assembled products may then pass through distribution centers in South and Central America to retail locations across the United States. This circuitous production path complicates the accuracy of trade data, as recent studies have shown, as well as the process of supplier management and supply chain tracing. Not only is it difficult to calculate the value added during each manufacturing step, but it is difficult to assess the risks associated with each new component supplier and contract manufacturer in the supply chain.

In addition, it is increasingly difficult for analysts to independently understand the nature of ICT supply chains. As little as 5–10 years ago, data from transactional information sources could trace ICT shipments from component producers in mainland China and Taiwan to manufacturing centers in North and South America. However, as the emerging middle class in China consumed more ICT technologies, China, Hong Kong, and Taiwan became favored locations for ICT firms' production facilities.[14] In China especially, government subsidies and policies requiring relocation in exchange for market access further encouraged multinationals to establish subsidiaries and joint ventures on the mainland. The establishment of multinational subsidiaries in East Asia has made independent open source supply chain analysis more difficult. Often the biggest supplier for many U.S. ICT companies, especially the larger ones, is their own East Asian subsidiary. For example, the largest supplier for Intel-Mexico, Intel-Colombia, and Intel-USA is Intel-Shanghai. Identifying the secondary and tertiary suppliers that contribute products and value early in the supply chain can be challenging due to the lack of transparent documentation and constantly changing business relationships. **Exhibit 2** provides an example of this phenomenon.

[11] Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

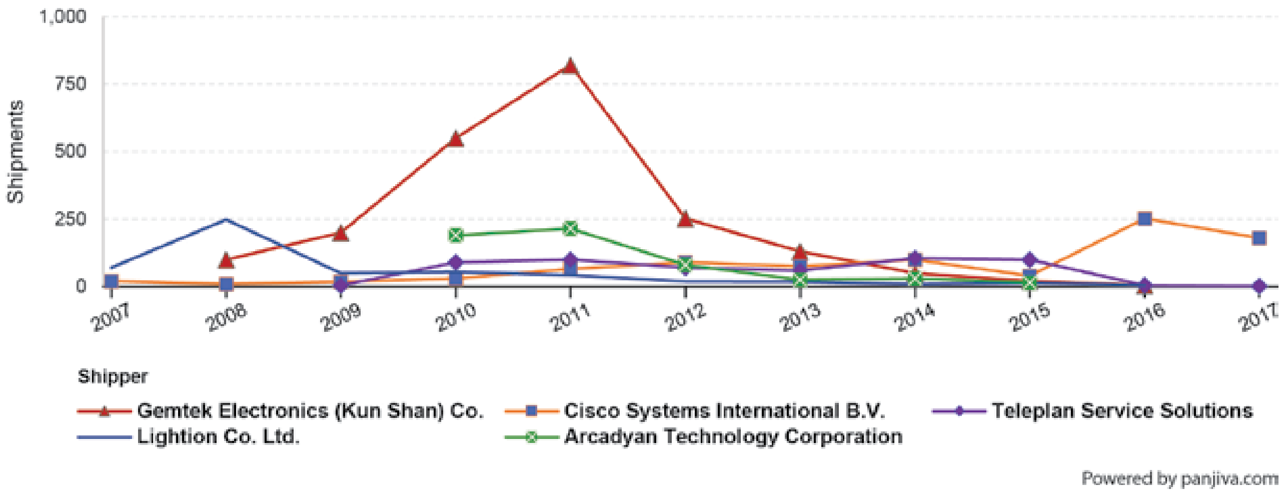
[12] U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations" (GAO-17-688R State Department Telecommunications, July 27, 2017), https://www.gao.gov/assets/690/686197.pdf.

[13] Greg Linden, Kenneth L. Kraemer, and Jason Dedrick, "Who Captures Value in a Global Innovation Network? The Case of Apple's iPod," *Communications of the ACM* 52, no. 3 (March 2009): 140–44, http://pcic.merage.uci.edu/papers/2008/whocapturesvalue.pdf.

[14] Organisation for Economic Co-operation and Development (OECD), *OECD Science, Technology and Innovation Outlook 2016* (Paris: OECD Publishing, 2016), http://dx.doi.org/10.1787/sti_in_outlook-2016-en.

Exhibit 2

Annual Shipments by Suppliers to Cisco Systems, 2007–2017



Source: Panjiva.

Exhibit 2 shows the year-to-year shift in Cisco's U.S. import registered supplier data, as shipments from Gemtek Electronics (Kun Shan) Co. Ltd. (China), Arcadyan Technology Corporation (Taiwan), and Lightion Co. Ltd. (Hong Kong) gradually disappear from the data set and are replaced by shipments from Cisco Systems International B.V., a subsidiary based in the Netherlands that appears to manage Cisco's international shipments. This trend effectively masks the deeper levels of Cisco's supply chain, making it less clear which East Asian companies are serving as third- and fourth-tier suppliers.

A similar pattern is evident among the other top enterprise IT providers to the federal government. HP's top two suppliers of China-origin goods are its own subsidiaries in Singapore and Mexico. Unisys's primary shipper of China-origin products is Unisys C O Exel, which began shipping from China to Unisys subsidiaries in Mexico and Colombia around 2012. For Intel, Microsoft, Cisco, Boeing, and IBM, the top supplier of China-origin items is the company itself.

The practice of sourcing primarily from foreign subsidiaries can make it more difficult to determine the primary component suppliers in a supply chain, and this lack of transparency is itself an added source of risk. This is because for SCRM, both the location of the production and the entity in control of that production are important factors in assessing risk. Risks associated with location and control of production exist along a spectrum, and can be aggravated or mitigated by other factors. Production by a Chinese state-owned enterprise (SOE) based in China presents greater risk to the federal ICT supply chain than production by a Singaporean firm based in China, yet both present more risk than a Singaporean firm based in Singapore. This is because production based in sensitive countries or in countries known for counterfeiting and intellectual property (IP) violations poses heightened risk regardless of who does the manufacturing. Due to reliance on foreign legal, political, and financial systems and labor markets, as well as the infrastructure of a foreign nation, foreign subsidiaries may be at greater risk of penetration by nefarious actors than domestic subsidiaries and a company's recourse in the event of penetration may be more limited. In China in particular, companies involved in trade disputes or corporate litigation can encounter difficulties obtaining records or serving subpoenas that would allow prosecution, and must prove they have taken steps to properly safeguard trade secrets in order to successfully sue.[15]

[15] Del Quentin Wilber, "Stealing White: How a Corporate Spy Swiped Plans for DuPont's Billion-Dollar Color Formula," Bloomberg, February 4, 2016, https://www.bloomberg.com/features/2016-stealing-dupont-white/.

The entity in control of production also factors into the analysis. A parent company has most control over location security, staff hiring, manufacturing, and quality control practices at domestic subsidiaries. Depending on a company's corporate culture and internal controls, that same company may have more control at a foreign subsidiary than it would at a foreign third-party manufacturer. Apple, for instance, has instituted strict controls at its production sites in China in an effort to secure its supply chain and protect its IP.[16] However, the foreign subsidiary may still be subject to foreign regulations or influence in ways that increase risk related to a company and its products.

[16] William Turton, "Leaked Recording: Inside Apple's Global War on Leakers," *The Outline*, June 20, 2017, https://theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers.

Chapter 2: SCRM Laws, Regulations, and Other Requirements

Supply chain risk management is an important component of a comprehensive cybersecurity mission, but it also has a role in market research, acquisitions, and procurement, as well as broader programmatic activities such as program lifecycle planning. A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, as the following sections will show, SCRM of federal ICT systems has been divided in multiple ways—among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems.

FEDERAL INFORMATION SYSTEMS AND NIST

The OMB has purview over federal information systems "used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency."[17] NIST creates standards and guidelines for these systems. NIST is not a regulatory agency; rather, it develops security standards and guidelines through a comprehensive public review process. For many products, this process involves three cycles of public vetting, during which comments on draft publications are solicited from individuals and organizations in the public and private sectors.[18] NIST's outreach efforts encourage feedback and discussion, particularly from owners, operators, and administrators of the information systems for which NIST sets standards. This process aims to ensure that the guidelines are both technically correct and implementable.

In 2002, Congress passed the Federal Information Security Management Act (FISMA), which required NIST to develop security standards and guidelines to protect federal information systems and allowed the OMB to make NIST standards compulsory and binding.[19] NIST's FISMA Implementation Project was established in 2003 to produce the required security standards and guidelines for federal information systems; its publications include Federal Information Processing Standards (FIPS) 199, FIPS 200, and the NIST Special Publications (NIST SP) 800 series.

Neither FIPS 199 (2004) nor FIPS 200 (2006) mention supply chain issues. FIPS 199 focuses on categorization, creating the requirement to rate information systems as low, moderate, or high impact in terms of confidentiality, integrity, and availability.[20] FIPS 200 sets some minimum security requirements in the areas of access control, awareness and training, configuration management, media protection, personnel security, resource allocation, and licensing policy, among others. FIPS 200 also introduced the concept that risk management includes "continuous" or "ongoing" monitoring of the security state of the information system.[21]

The FIPS 199 categorizations and policies are used to determine which systems are subject to enhanced cybersecurity measures and SCRM requirements, but the FIPS standards do not require SCRM of those systems, or specify the scope or extent of supplier due diligence that should be used in evaluating products, services, or suppliers of those systems. The FIPS 200 controls are designed to mitigate threats posed by individuals who are improperly trained or credentialed, and to avoid resource management errors that may result in an improperly disposed hard drive or an improperly used or licensed software program. They are not designed to mitigate risk posed by ICT products that may have been compromised during the manufacturing, programming, or deployment process. This separation is intentional. Supplemental information released with FIPS 200 in March 2006 explained that during the review

[17] "Circular No. A-130: Managing Information as a Strategic Resource," Office of Management and Budget, July 28, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

[18] "FAQs: General Questions, National Institute of Standards and Technology," Computer Security Resource Center, updated October 18, 2017, http://csrc.nist.gov/groups/SMA/fisma/faqs.html.

[19] This means that standards created under the authority of Sections 20(a) and 20(b) of the National Institute of Standards and Technology Act 15 U.S.C. 278g–3(a) were mandatory.

[20] National Institute of Standards and Technology, *FIPS PUB 199*.

[21] National Institute of Standards and Technology, *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

process NIST had received comments suggesting "additions and changes to the standard concerning risk management procedures, audit controls, baseline security controls, and risks introduced by new technologies," all of which could be considered SCRM-related. NIST's response to this comment indicated that these elements were best addressed in forthcoming NIST SP 800-53, and ultimately aggregated from across all NIST SPs in SP 800-161, rather than updated in the FIPS 199 and 200 series.[22] The result of this decision is that while FIPS 199 and 200 controls are legally mandated, the SCRM-related controls in NIST SPs remain merely guidance. A stronger legal or regulatory requirement relating to SCRM could help bridge this gap. That said, it is not—nor should it be—the role of NIST to enforce stronger legal or regulatory requirements, as this would severely diminish NIST's value as convening entity.

NATIONAL SECURITY SYSTEMS AND THE CNSS

Policies for NSS are controlled by the Committee on National Security Systems (CNSS). The CNSS is an interagency body chaired by the Department of Defense (DoD) and the U.S. military, with membership from the intelligence community, the DHS, the Department of Justice, and other entities. The CNSS was formed in 2001 by Executive Order 13231; it evolved from the National Security Telecommunications and Information Systems Security Committee, which had been created in 1990. The executive agency for the CNSS is the National Security Agency (NSA).

The Federal Information Security Management Act of 2002 defines NSS as follows:

> *(2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—*
>
> *(i) the function, operation, or use of which—*
>
> *(I) involves intelligence activities;*
>
> *(II) involves cryptologic activities related to national security;*
>
> *(III) involves command and control of military forces;*
>
> *(IV) involves equipment that is an integral part of a weapon or weapons system; or*
>
> *(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or*
>
> *(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.*
>
> *(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).*[23]

Or, as the DoD explains, an NSS is—

> *A telecommunications or information system operated by the Federal Government that involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or that is critical to the direct fulfillment of military or intelligence missions.*[24]

[22] National Institute of Standards and Technology, *Announcing Approval of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), https://www.federalregister.gov/documents/2006/03/31/E6-4720/announcing-approval-of-federal-information-processing-standard-fips-200-minimum-security.

[23] FISMA, Pub. L. No. 107-347, Title III (December 17, 2002).

[24] Inspector General, Department of Defense, "DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems" (Report No. DODIG-2016-123, Department of Defense, Alexandria, VA, August 15, 2016), http://www.dodig.mil/pubs/documents/DODIG-2016-123.pdf.

Thus, NSS encompass more than military or intelligence systems, or various levels of classified information.[25] For example, the Department of Energy has NSS by virtue of its mission to maintain the nuclear weapons stockpile. Similarly, other agencies including the Departments of Energy, State, Treasury, and Justice all have roles in intelligence, a mission not limited to agencies such as the Central Intelligence Agency and the DoD.

Although the CNSS was established to develop operating policies, procedures, guidelines, instructions, and standards for NSS, FISMA specifically grants the Secretary of Defense and the Director of Central Intelligence separate, individual authority over their own systems. As stated in a 2002 House Committee on Government Reform report, "This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements."[26]

EXECUTIVE BRANCH AND SCRM

Congress is not alone in its ability to influence NIST and federal ICT policy; actions by the Executive Branch have advanced the ICT and SCRM agenda in important ways.

The Comprehensive National Cybersecurity Initiative was established by President George W. Bush in January 2008 through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and expired under President Barack Obama.[27] The directive established the foundation for current DoD policy on cybersecurity issues and provided the initial impetus to the DoD's SCRM efforts by including funding for pilot programs and reports on results, elements of which were the basis for subsequent comprehensive enterprise SCRM programs. The directive called for the Secretaries of Defense and Homeland Security, in coordination with the Secretaries of the Treasury, Energy, and Commerce; the Attorney General; the Director of National Intelligence; and the Administrator of General Services, to develop a strategy and implementation plan to, among other issues, "better manage and mitigate supply chain vulnerabilities," including specific recommendations for the federal government and defense acquisition process. The CNCI itself aimed to reduce federal ICT vulnerabilities and prevent intrusions; strengthen supply chain security; and enhance research, development, education, and investment in key technologies. The DHS and DoD were the lead agencies for the SCRM initiative, but the directive and its related activities remained classified. A March 2010 report on the initiative by the Government Accountability Office noted that the classification level hindered efforts by the Department of State and the National Cyber Security Center to engage outside organizations, including the private sector.[28]

In March 2010, the DoD issued DoD Directive-Type Memorandum 09-016–SCRM to Improve the Integrity of Components Used in DoD Systems. The directive defined SCRM and supply chain risk, and stated that supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

[25] Further details on the connection between NSS and classified information can be found in National Security Agency, *CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems* (Ft. Meade, MD: CNSS Secretariat, March 2014), http://www.dss.mil/documents/CNSSI_No1253.pdf; and National Security Agency, *CNSSI No. 1253 Attachment 5: Classified Information Overlay* (Ft. Meade, MD: CNSS Secretariat, May 2014), http://cryptome.org/2014/05/cnss-classified-info-overlay.pdf.

[26] National Institute of Standards and Technology, *NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System* (Gaithersburg, MD: Computer Security Division, August 2003), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf; U.S. House of Representatives, "Report of the Committee on Government Reform" (Report 107-787, November 14, 2002), 85, quoted in NIST Special Publication 800-59.

[27] "National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23," The White House, (Washington, DC, January 8, 2008, https://www.georgewbushlibrary.smu.edu/~/media/GWBL/Files/Digitized%20Content/2014-0390-F/t030-021-012-nspd54-1-20140390f.ashx.

[28] U.S. Government Accountability Office, "Cybersecurity: Progress Made by Challenges Remain in Devining and Coordinating the Comprehensive National Initiative" (GAO-10-338, Washington, DC, March 2010), http://www.gao.gov/new.items/d10338.pdf.

Directive-Type Memorandum 09-016 was subsumed in November 2012 by DoD Instruction 5200.44, which was modified by Change 1 in August 2016.[29] The 2012 Instruction considers National Security Presidential Directive 54/Homeland Security Presidential Directive 23 the basis for the directive's SCRM implementation strategy, along with the following references:

- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008
- Section 806 of Public Law 111-383, "The National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
- DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008 (updated January 7, 2015)
- DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (from DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002)
- Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management (SCRM)," March 7, 2012[30]

Military and intelligence systems are a subset of NSS, rather than the other way around, and DoD SCRM policies have largely been developed by the DoD itself, or by the DoD in concert with other members of the CNSS.

In 2013, President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," provided an influential but unanticipated boost to SCRM policy. The executive order focused on improving the cybersecurity of "Section 9 entities," or "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[31] The order does not mention supply chain or SCRM, but it tasks NIST with creating "a framework to reduce cyber risks to critical infrastructure," including "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." This framework would become the NIST Cybersecurity Framework (NIST CSF).

The NIST CSF, published in February 2014, created the Identify, Protect, Detect, Respond, and Recover framework now ubiquitous throughout federal discussions of cybersecurity.[32] Supply chain issues make a brief appearance in the Business Environment category of the Identify section of the framework, which instructs organizations to identify their role in the supply chain. The framework highlights NIST SP 800-53 Rev. 4 as an informative reference for this subcategory. Other SCRM developments continued gradually from previous lines of effort, as when a revision to NIST SP 800-37, released in June 2014, briefly mentioned SCRM with respect to external providers of ICT products.[33] The NIST CSF now underpins much of the discussion surrounding federal ICT cybersecurity, and thus SCRM, for federal ICT networks. Despite the framework's origins as an effort focused on critical infrastructure, it has been adopted by numerous federal organizations.

[29] Department of Defense, "Department of Defense Instruction 5200.44" (August 25, 2016), https://www.hsdl.org/?abstract&did=795012.

[30] National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, March 7, 2012), https://info.publicintelligence.net/CNSS-SupplyChainRisk.pdf.

[31] The White House, "Executive Order–Improving Critical Infrastructure Cybersecurity" (Office of the Press Secretary, Washington, DC, February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[32] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[33] National Institute of Standards and Technology, *NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Live Cycle Approach* (Gaithersburg, MD: Computer Security Division, February 2010), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

CONGRESSIONAL ACTION AND SCRM

The Federal Information Technology Acquisition Reform Act (FITARA), FISMA, and the Cybersecurity Enhancement Act currently delineate the bounds of debate surrounding federal ICT risk management.

Federal Information Technology Acquisition Reform Act

Although introduced in 2013, the final version of FITARA did not become law until late 2014, when it passed as part of the FY 2015 National Defense Authorization Act.[34] FITARA had seven primary focus areas:

1. Enhancing the authority of the chief information officer
2. Enhancing transparency and improved risk management in IT investments
3. Requiring savings through IT portfolio review
4. Expanding the training and use of IT cadres
5. Consolidating federal data centers
6. Maximizing the benefit of the Federal Strategic Sourcing Initiative
7. Expanding government-wide software purchasing programs

FITARA tasked the OMB with implementing a process for ICT portfolio review and reviewing ICT acquisition staffing demands. FITARA was passed with fiscal concerns in mind and is commonly understood as an attempt to properly plan and manage incredibly expensive IT acquisitions. Congress views FITARA primarily as a fiscal oversight initiative designed to prevent costly spending, rather than as a security policy. Conversations between Interos leadership and congressional offices revealed Congress is reluctant to securitize FITARA by adding SCRM elements to the policy, such as requiring baseline vendor vetting prior to approving acquisitions. However, like previous policy efforts, FITARA has affected supply chain issues indirectly.

FITARA helps federal chief information officers increase visibility over their ICT infrastructure, potentially reducing vulnerabilities due to lack of oversight and transparency of what systems exist and therefore need some aspect of security. Perhaps somewhat paradoxically, however, FITARA's focus on portfolio review encourages agencies to identify aging infrastructure elements and consolidate them through new technologies. Portfolio review encourages modernization, and modernization introduces new COTS products into federal ICT systems. Due to the nature of global ICT supply chains, most new products that will enter federal ICT systems will include components originating in China or produced by Chinese firms. The use of COTS presents some challenges, given the confidentiality, integrity, and accessibility requirements for federal systems. In September 2017, FedScoop announced the results of a survey of 200 federal IT executives conducted by Unisys Corporation and the research company Market Connections. Fifty-nine percent of survey respondents said IT modernization efforts have increased the cybersecurity challenges they face.[35]

A lack of compliance with FITARA can be an indicator of cybersecurity vulnerabilities resulting from aging and poorly maintained ICT infrastructure, including vulnerabilities originating from supply chain risks. More important, a chief information officer's limited oversight of their federal IT systems creates potential gaps in security. This said, compliance with FITARA does not itself directly equal achieving comprehensive cybersecurity or oversight of a federal ICT supply chain.

The Modernizing Government Technology Act could place similar pressure on federal agencies. The bill was introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016.[36] The act creates a $500 million central modernization fund that agencies can

[34] Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, H.R. 3979, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/3979.

[35] Carten Cordell, "IT Modernization Efforts Increase Cybersecurity Challenges, Survey Says," FedScoop, September 6, 2017, https://www.fedscoop.com/survey-modernization-efforts-increasing-cybersecurity-challenges/.

[36] Modernizing Government Technology Act of 2016, H.R. 6004, 114th Cong. (2015–2016), https://www.congress.gov/bill/114th-congress/house-bill/6004.

borrow against to update aging IT systems.[37] The act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The bill was amended to the Senate version of the National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.[38]

The Modernizing Government Technology Act seems to presume that legacy equipment and systems are the sole source of risk, and that this risk can be mitigated through modernization. But modernization will actually increase risk if newly adopted technologies are not assessed appropriately before being integrated into federal IT networks. The bill establishes responsibilities and financial rewards to the agencies for modernizing their IT infrastructure and names the OMB and GSA as permanent members of a supervisory board, but it does not require any measure of supply chain security as part of modernization efforts. In the memorandum on "Implementation of the Modernizing Government Technology Act" signed by OMB Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for SCRM as part of an agency's request for modernizing funds.[39]

As federal agencies face additional pressure from efforts like FITARA and the Modernizing Government Technology Act, the need for robust ICT SCRM leadership as well as an appropriately resourced capability becomes ever more important, affecting the ICT products agencies acquire, how and at what speed they acquire them, the suppliers they use, and the eventual quality and security over the product lifecycle.[40]

Federal Information Security Modernization Act and Circular A-130

FISMA sought to centralize federal cybersecurity management with the DHS, retaining the OMB's authority over policies for federal information systems but charging the DHS with the implementation of those policies. The bill retained the prerogatives of the Secretary of Defense and the Director of National Intelligence for their own systems. Although FISMA 2014 required continuous cybersecurity monitoring, sparking the DHS-led Continuous Diagnostics and Mitigation program, FISMA did not address SCRM specifically, creating yet another gap in federal laws and regulations.

The passage of FISMA 2014 also tasked NIST with continuing its work to protect federal information systems. In April 2015, NIST released SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," the most detailed NIST contribution to the SCRM discussion since the creation of Control SA-12 in 2010. NIST SP 800-161 adopted the definition of risk from FIPS 200 to establish a definition for ICT supply chain risk and built on NIST SP 800-53 Rev. 4 and NIST Interagency Report 7622, *National Supply Chain Risk Management Practices for Federal Information Systems*, to enhance the overlay of ICT-specific SCRM controls.[41]

The OMB incorporated the new FISMA requirements and NIST controls into active policy. In support of FISMA 2014, the OMB issued Circular A-123 and revised Circular A-130 in July 2016. Circular A-123 broadened the scope of risk management beyond fiscal compliance and required federal organizations to establish an enterprise risk management capability, of which A-130 and SCRM are key components.[42] The release of a revised Circular A-130

[37] National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/2810.

[38] Jason Miller, "In the End, Senate Lets the MGT Act in the Defense Bill," *Federal News Radio*, September 19, 2017, https://federalnewsradio.com/legislation/2017/09/in-the-end-senate-lets-the-mgt-act-in-the-defense-bill/; Carten Cordell, "Trump Signs Modernizing Government Technology Act into Law," FedScoop, December 12, 2017, https://www.fedscoop.com/trump-signs-mgt-act-law/.

[39] The White House, "M-18-12, OMB Memorandum, Implementation of the Modernizing Government Technology Act" (Washington, DC: Office of Management and Budget, February 27, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf

[40] "The Importance of SCRM's Role in Connection to FITARA," Interos Solutions, February 9, 2015, https://interosblog.wordpress.com/2015/02/09/the-importance-of-scrms-role-in-connection-to-fitara/.

[41] National Institute of Standards and Technology, *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Gaithersburg, MD: Computer Security Division, April 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

[42] KMPG International, "A-123 Aims to Strengthen Government with Enterprise Risk Management," Government Executive, January 5, 2017. http://www.govexec.com/govexec-sponsored/2017/01/-123-aims-strengthen-government-enterprise-risk-management/134386/; The White House, "M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control" (Washington, DC: Office of Management and Budget, July 15, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf.

was key, as it had not been updated since 2000.[43] The circular expanded on risk management issues and included specific supply chain security language. Perhaps most important, the circular requires agencies to implement security policies issued by the OMB, including standards and guidelines contained in NIST products, and formally establishes a shift from three-year review and authorizations of compliance activities to continuous monitoring of those activities. Appendix I of the circular details general requirements, implementation of FITARA, and SCRM principles.[44] The circular requires agencies to develop SCRM plans as described in NIST SP 800-161 and to satisfy the information security requirements in FIPS 200 and the security control baselines in NIST SP 800-53. It should be noted that as of the writing of this report, there has been no known audit to ensure federal agencies have impactful SCRM programs in place, nor is there policy that mandates a government-wide national supply chain risk management strategy.

Cybersecurity Enhancement Act

As part of the implementation of President Obama's Executive Order 13636, Congress modified NIST's mission in the Cybersecurity Enhancement Act of 2014, to have NIST continue work on the CSF and expanded the use of the CSF to owners and operators of critical infrastructure.[45]

This call for owners and operators of critical infrastructure to take NIST's work into account appears to be part of a broader move toward consolidating parts of the federal ICT policy framework. DoD Instruction 8500.01, issued in March 2014, required the DoD to implement system security controls designed by NIST, but it is DoD Instruction 5200.44, Change 1, effective August 2016, that explicitly adds NIST SP 800-161 as a basis for the implementation of the DoD SCRM strategy. Similarly, the CNSS released a revision of CNSS Directive 505, "Supply Chain Risk Management," in August 2017, replacing the directive published in March 2012.[46] The new directive makes explicit connections between the CNSS and NIST, explaining that the CNSS adopts NIST standards where applicable and publishes additional guidelines in instances where NIST does not sufficiently address the needs of NSS.

A new revision of the CSF was released for comment in January 2017, providing new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity. It also includes references to SCRM across all five components of the framework.[47] Increasingly integrating SCRM into federal risk management efforts is important to successfully managing the ICT modernization efforts envisioned in legislation like FITARA, but there remains no centralized leadership for federal SCRM efforts. Additionally, existing regulations and requirements do not adequately address the risk posed by COTS products, or risks related to ICT products linked to China or other state actors that may pose a threat to the United States.

[43] The White House, "M-16-17."

[44] Jason Miller, "OMB Initiates Cyber Marathon with Long-Awaited Policy Update," *Federal News Radio*, October 21, 2015, https://federalnewsradio.com/omb/2015/10/omb-initiates-cyber-marathon-long-awaited-policy-update/.

[45] Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353/text; "NIST Releases Update to Cybersecurity Framework," National Institute of Standards and Technology, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

[46] National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, July 26, 2012), https://1yxsm73j7aop3quc9y5ifaw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/CNSSD_505_Final2-Published-08-01-2017.pdf.

[47] "NIST Releases Update," National Institute of Standards and Technology.

Chapter 3: Supply Chain Analysis of Federal ICT Manufacturers

As previously stated, this study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. The reason for this, as outlined below, is that the greatest risks are often unknown and driven directly by the location of the multiple tiers of suppliers and the nature of their third-party affiliations.

SUPPLIER LOCATION

No laws or regulations mandate that federal IT suppliers provide multi-tier transparency regarding their supply chains; however, HP, Dell, and Microsoft have embraced industry transparency principles in a way that allows some insight into their first-tier suppliers. All three publish lists of their primary suppliers, a practice that is not standard across the industry.[48] The lists are not constructed identically, so the data require some manipulation before they can be analyzed. Dell provides site addresses for all of its tier-one suppliers; HP provides site addresses for its final assembly suppliers but not for its commodity and component suppliers; and Microsoft provides a list of the names of its top 100 suppliers.[49]

For this paper, Interos analyzed the publicly reported supplier networks of HP, Dell, and Microsoft. Of the 344 identified suppliers for HP, Dell, and Microsoft, it was possible to identify a site address for 212. The 132 suppliers for which a site address could not be identified were categorized according to the location of their corporate headquarters. As expected, HP, Dell, and Microsoft source from the same companies; at times from the same company at the same site. As an example, all three source from Pegatron Corporation. Dell identified two site addresses from which it does business with Pegatron—one in Taoyuan City, Taiwan, and one in Jiangsu, China. HP also reported sourcing from the Jiangsu site. Because Microsoft reported sourcing from Pegatron, but did not identify a site, Microsoft was categorized as sourcing from Pegatron's headquarters in Taipei, Taiwan. Thus, the combined supplier list includes three entries for Pegatron: one for Taoyuan City, Taiwan; one for Jiangsu, China; and one for the Taipei, Taiwan headquarters. Using this categorization system, the unified suppliers list identifies 39 percent of suppliers to these three companies as located in China, 15 percent located in Taiwan, 13 percent located in the United States, and 8 percent located in Japan.

The links to China are more numerous than these data suggest, because a number of companies were categorized only by the location of their company headquarters. For the 132 companies for which a site address could not be conclusively determined, 87 were headquartered in Taiwan, the United States, or Japan. The unified supplier list categorizes these 132 suppliers only by the location of their headquarters, not by any supplier sites that may be elsewhere, yet it is common for companies headquartered in Taiwan, the United States, Japan, and other countries to base their production facilities in China. It is likely that a significant portion of these companies have operations in China, making China's influence on these supply chains larger than it appears at first glance.

SUPPLIER FINANCING AND INFLUENCE

Financial links to suspect entities, including state-owned or substantially state-controlled enterprises, are also important for SCRM, as they indicate potential vectors for nefarious influence. Previous reports have raised concerns about the connections between Intel, HP, Dell, IBM, Cisco, Microsoft, and Chinese entities such as

[48] Apple follows similar transparency policies. Apple is a not a top 10 provider of enterprise ICT to the U.S. federal government, however, so its data were not included in this analysis.

[49] Nick Wingfield and Charles Duhigg, "Apple Lists Its Suppliers for 1st Time," The New York Times, January 13, 2012, http://www.nytimes.com/2012/01/14/technology/apple-releases-list-of-its-suppliers-for-the-first-time.html; "HP Suppliers," Hewlett-Packard, http://h20195.www2.hp.com/V2/GetPDF.aspx/c03728062.pdf; "Our Suppliers," Dell, About Dell, Corporate Social Responsibility, Supply Chain, http://www.dell.com/learn/us/en/uscorp1/cr-social-responsibility; "Microsoft Top 100 Production Suppliers," Microsoft, http://download.microsoft.com/download/0/1/4/014D812D-B2E3-43A0-A89A-16E3C7CD46EE/Microsoft_Top_100_Production_Suppliers_2016.pdf.

Tsinghua Holdings, Inspur Group, Beijing Teamsun Technology, and the China Electronics Technology Group Corporation (CETC).[50] In the analysis of suppliers for HP, Dell, and Microsoft, 28 suppliers (that accounted for 52 supplier site locations) were identified as presenting some level of risk owing to their connections to Chinese state-owned entities. **Table 2** includes information on several of these entities of concern. Risk can be present in the nature of the government's relationship with an entity: "state-controlled" entities listed below function in some ways as part of official government or military institutions; "state-owned" entities have significant financial ownership or control by the state; "state-influenced" entities may have other, less formal, ties to a government, such as strategic partnerships or leadership connections; and "defense suppliers" provide services or products to a state's government, military, or security services.

For this report, Interos complied a listing of entities, their potential risk based on the relation to the Chinese government, and the publicly available sources this information was garnered from. Further research would need to be completed to truly understand the comprehensive risk these entities may pose to U.S. ICT supply chains.

Table 2
Examples of Federal ICT Suppliers Connected to Entities of Concern

Entity Name	Risk	Details	Source
Beijing Teamsun Technology	Defense supplier	Partnership with IBM.	Various.
BOE Global	State-owned	Supplies display/liquid crystal display to Dell.	15.24 percent owned by Beijing State-Owned Assets Supervision and Administration.
China Electronics Technology Group Corporation (CETC)	State-controlled Defense supplier	A network of former military labs that operates both commercial and military technology businesses. Strategic partnerships with Microsoft and IBM.	State-owned company according to Dow Jones.
Chinese Academy of Sciences (CAS)	State-controlled	Connections to Chinese military, nuclear, and cyberespionage programs. Often appears as an investor or partner of other Dell, HP, or Microsoft suppliers.	Various.
Huawei	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.
Inspur Group	Defense supplier	Joint ventures and partnerships with Cisco, Intel, and IBM.	Various.
Legend Capital/ Holdings	State-controlled	Asset management arm of the CAS, and the owner of Lenovo. Occasionally appears as an investor or partner of other Dell, HP, or Microsoft suppliers. Part of a consortium that acquired Lexmark in 2016.	Various.
Lenovo	State-owned	Cyberespionage risk.	29.10 percent owned by Legend Holdings Corp.
Lexmark	State-influenced	Acquired in April 2016 by a consortium including Legend Capital. History of security vulnerabilities. Supplies accessories/printers to Dell.	Various.
Lishen Power Battery Systems Co. Ltd.	State-owned	CETC is sole shareholder. Supplies batteries to Dell.	State-owned company according to Dow Jones.
Tianma Microelectronics (USA) Inc. .	State-owned	Owned by China defense supplier. Supplies displays to Microsoft	20.81 percent owned by AVIC International Holdings Ltd. and 11.35 percent owned by the State-Owned Assets Supervision and Administration Commission.

[50] "U.S. Tech Companies and Their Chinese Partners with Military Ties," *The New York Times*, October 30, 2015, https://www.nytimes.com/interactive/2015/10/30/technology/US-Tech-Firms-and-Their-Chinese-Partnerships.html.

Entity Name	Risk	Details	Source
TPV Technology Ltd.	State-owned	Supplies display/liquid crystal display to Dell and HP.	37.05 percent owned by the State-Owned Assets Supervision and Administration Commission.
Tsinghua Holdings	State-controlled	Asset management group focused on technology and defense sector. Joint ventures and strategic partnerships with Intel, HP, Dell, and IBM.	State-owned company according to Dow Jones.
Shenzhen Laibao Hi-Tech Co. Ltd	State-owned	Supplies display/liquid crystal display to Dell and HP.	20.91 percent owned by the State-Owned Assets Supervision and Administration Commission.
Zhongxing Telecommunications Corporation	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.

Source: Interos Solutions.

Entities that present the most risk to the supply chain are those that exhibit close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs. For example:

- Dell supplier Lishen Power Battery Systems Co. Ltd. is a subsidiary of Tianjin Lishen Battery Joint-Stock Company Limited, an SOE affiliated with CETC, which is a network of former military labs that operates both commercial and military technology businesses. CETC appears to be Lishen's sole shareholder.[51]

- Hengdian Group DMEGC Magnetics Co. Ltd. supplies magnetic materials to Microsoft, and is a subsidiary of Hengdian Group Holdings. The group's website states it is an enterprise approved by the Chinese Academy of Sciences (CAS) and China's Ministry of Science and Technology, and has cooperated with the state-owned China National Nuclear Corporation.[52]

- GoerTek Inc. supplies acoustic components to Microsoft. In addition to state-backed investment from China International Fund Management Co., Ltd., the company has long-term strategic partnerships with the CAS and universities linked to China's cyberespionage programs, such as Tsinghua University, Zhejiang University, and Harbin Institute of Technology.[53] Other customers include Lenovo.[54]

The connections between these firms and entities involved in China's military, nuclear, or cyberespionage programs increase risk associated with federal ICT providers sourcing products or services from these firms. This risk could present itself as a supply chain attack through a compromised product, such as batteries or acoustic components supplied to federal ICT providers. Still other Chinese SOEs supply federal ICT providers with magnets, shielding materials, or cables and power connectors.[55] These products could present risk if they are of inferior quality and fail to operate, but they are unlikely to present significant cybersecurity risk to federal ICT networks. The risk might also stem from more subtle actions, including by federal ICT providers revealing design information, product specifications, or other sensitive information to their suppliers as part of standard business practices. Business information that may be innocuous when passed to a standard business partner becomes less innocuous when passed to individuals or entities associated with a rival government.

A good SCRM program assesses the risks associated with the nature of a particular product in tandem with the risks stemming from the entity that is producing or providing the product. Assessing the supply chain risks associated with liquid crystal displays (LCDs) is one example of this process. Displays are not as critical to an end-product

[51] "Shareholder's Info," Lishen, About Lishen, accessed October 29, 2017, http://en.lishen.com.cn/textContent.aspx?cateid=181&bigcateid=171.
[52] "History," Hengdian Group, About Us, accessed March 23, 2018, from Internet Archive WayBackMachine, https://web.archive.org/web/20170415230303/http://www.hengdian.com/site/en/en_com_history.htm.
[53] "Partners," Goertek, About Us, accessed March 23, 2018, http://www.goertek.com/en/about/hzhb.html.
[54] "Goertek Announces Next-Gen VR Reference Design Powered by Snapdragon™ 845," PRNewswire, March 2, 2018, https://www.prnewswire.com/news-releases/goertek-announces-next-gen-vr-reference-design-powered-by-snapdragon-845-300607312.html.
[55] "HP Suppliers," Hewlett-Packard; "Our Suppliers," Dell; "Microsoft Top 100 Production Suppliers," Microsoft.

as its microprocessor, but their hardware, firmware, and connections to other ICT products can make them an important component in an ICT supply chain. In 2016, security researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their monitor displays.[56]

Several Chinese companies manufacture the LCDs that are a component of tablets, notebooks, and other computers produced by Microsoft, Dell, HP, and other federal ICT providers, and several of these companies have ties to the Chinese government or military. For example:

- Tianma Microelectronics supplies LCDs to Microsoft. The company's primary shareholders include AVIC International Holdings Ltd., the State-Owned Assets Supervision and Administration Commission (which manages the central government's SOEs), and the City of Wuhan. AVIC is an SOE that was formed in 2008 after the consolidation of China Aviation Industry Corporation I (AVIC I) and China Aviation Industry Corporation II (AVIC II).[57] AVIC is also one of China's largest defense suppliers, and makes aircraft for civilian and military uses, including bombers and fighter jets.

- Dell and HP both source LCDs from the state-owned TPV Technology Ltd. and Shenzhen Laibao Hi-Tech Co. Ltd. TPV Technology Ltd. is a China-based company that also does business as Top Victory Electronics Company and TPV-INVENTA Technology Co., Ltd. The company is controlled by state asset groups such as the State-Owned Assets Supervision and Administration Commission and China Greatwall Technology Group Co., Ltd. The State-Owned Assets Supervision and Administration Commission also controls 20 percent of Shenzhen Laibao Hi-Tech Co. Ltd. Dell also sources LCDs from six sites controlled by BOE Global, a company whose largest shareholder is the Beijing state-owned Capital Management Center.[58]

SUPPLY CHAIN RISK CASE STUDY: CORPORATE INTELLIGENCE-SHARING AGREEMENTS

An analysis of the business relationships of several top federal government ICT providers reveals corporate alliances and partnerships with SOEs in China as well as government-connected firms in Israel and Russia. Business relationships can affect multiple tiers within a single supply chain. While such networks of corporate alliance and partnership are common in the commercial sphere, they present security risks to federal ICT systems by potentially allowing nefarious actors access to technical information that could be used to infiltrate federal ICT systems. The information sharing inherent in commercial alliances can enable more efficient product integration and development. Commercial partnerships that share program application data, configuration information, or even deployment policies, however, may inadvertently grant malicious actors information they need to infiltrate federal ICT systems. Without a comprehensive SCRM program to investigate these partnerships, the connections and relationships may never be known, and the risk may remain undiscovered.

Intel and IBM: (In)Security Partnerships

Concerns associated with component production and manufacturing in China represent one facet of the supply chain risk facing the federal government's ICT system. As Chinese companies move up the value chain, the prospect of China-supplied software becomes ever more important to risk analysis. While an analysis of source code is generally not possible from unclassified sources, supply chain risks can be assessed on the basis of published business partnership announcements, including the establishment of corporate alliances.

Intel's Security Innovation Alliance allows partner companies to exchange threat intelligence and develop technology integrations with the McAfee Data Exchange Layer. The alliance produces integrated security solutions, by allowing technology partners to connect their products in a more efficient manner. The alliance includes companies (such as Huawei) with connections to the governments and security organizations of countries on

[56] Lorenzo Franceschi-Bicchierai, "Hackers Could Break into Your Monitor to Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016, https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.

[57] "Overview," AVIC, About Us, accessed October 29, 2017, http://www.avic.com/en/aboutus/overview/index.shtml.

[58] Lexis Nexis, Dun and Bradstreet, Dow Jones, Hoovers Data Repository. Factiva Database, Dow Jones and Reuters, New York.

the intelligence community's sensitive countries list.[59] As part of the alliance, Huawei provides a Cybersecurity Intelligence System that collects network traffic information in order to detect attacks and provide investigation and evidence collection capabilities. Huawei Cybersecurity Intelligence System works with McAfee ePolicy Orchestrator and McAfee Active Response. Partner products are subject to engineering testing prior to integration, but the risk in these partnerships stems from the possibility that information, source code, or other details shared as part of the product integration process could also be used to identify and exploit vulnerabilities in a product.

In a 2012 report, Gartner noted that the technical challenges of technology integration and corporate collaboration present increasing risk to ICT supply chains: "Enterprises are opening up their internal IT networks and systems to collaborate and share information with customers, partners and suppliers. As a result, all of these become targets for IT supply chain compromise."[60] Intel is not alone in participating in these sorts of alliances. In 2000, IBM announced a collaborative agreement with Huawei, including an R&D effort.[61]

VMware Partnerships with Chinese SOEs and Kaspersky

VMware, a subsidiary of Dell, has entered into corporate partnerships with Chinese SOEs that could present national security vulnerabilities to U.S. federal ICT systems. VMware provides cloud computing and software virtualization services to the U.S. government and the private sector. Following Dell's acquisition of VMware's parent company, EMC, in September 2016, Dell controls approximately 82.8 percent of VMware's outstanding common stock.[62]

In April 2016, VMware set up its first China joint venture with Sugon, a Tianjin-based company that specializes in high-performance computers, servers, storage products, and software systems. Sugon's full English name is Dawning Information Industry. It was founded as Dawning Yunjisuan Technology Co. Ltd. in 1996 with backing from the CAS. Currently the Chinese government is the largest shareholder of Sugon, with the CAS retaining a 23 percent stake.[63] The VMware-Sugon joint venture is called VMsoft and provides cloud computing and virtualization software and services. VMware holds a 49 percent stake in VMsoft, while Sugon holds a 51 percent stake.[64]

VMware also has product relationships with Kaspersky Lab,[65] the Russia-based cybersecurity and antivirus software company recently named in the DHS's divestment directive.[66] Kaspersky is a Russian-owned cybersecurity provider whose founder and CEO used to work for the KGB, the security service of the former Soviet Union.[67] A recent reported shift in the leadership of Kaspersky Labs has seen people with close ties to Russian military and intelligence services filling more executive positions. Speculation exists that these executives actually participate

[59] Warwick Ashford, "Check Point, Huawei Join Intel Security Innovation Alliance," *Computer Weekly*, November 3, 2016, http://www.computerweekly.com/news/450402310/Check-Point-Huawei-join-Intel-Security-Innovation-Alliance; "Huawei Joins Intel Security Innovation Alliance to Defend Customers against Security Threats," Huawei, News, November 4, 2016, http://www.huawei.com/en/news/2016/11/Huawei-Joins-Intel-Security-Innovation-Alliance; "McAfee Security Innovation Alliance Partner Directory," McAfee, Business Home, Partners, McAfee Security Innovation Alliance, accessed October 29, 2017, https://www.mcafee.com/us/partners/partnerlisting.aspx.

[60] "Maverick*Research: Living in a World without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned," Gartner, October 5, 2012, http://www.energycollection.us/Energy-Security/Living-World-Without-Trust-Filed.pdf.

[61] IBM, "IBM and Huawei Announce Networking Technology Collaboration," news release, September 25, 2000, https://www-03.ibm.com/press/us/en/pressrelease/1541.wss.

[62] VMware, Inc., "10-K Annual Report 2016," retrieved October 25, 2017, from SEC EDGAR database, https://www.sec.gov/Archives/edgar/data/1124610/000112461017000009/vmw-1231201610xk.htm.

[63] Tom Wilkie, "Chinese Government Kicks Commercial Companies Overseas," *Scientific Computing World*, August 25, 2015, https://www.scientific-computing.com/feature/chinese-government-kicks-commercial-companies-overseas.

[64] Jane Ho, "VMware Sets up First China Joint Venture with High-Performance Computer Maker Sugon," *Forbes*, May 24, 2016, https://www.forbes.com/sites/janeho/2016/05/24/VMware-sets-up-first-china-joint-venture-with-high-performance-computer-maker-sugon/#257d64db20af.

[65] "Kaspersky Agentless Virtualization Security," Kaspersky, Products, accessed October 30, 2017, https://usa.kaspersky.com/small-to-medium-business-security/virtualization-agentless; Department of Homeland Security, "DHS Statement on the Issuance of Binding Operational Directive 17-01," press release, September 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01; "Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 (2134021)," VMware, last updated October 16, 2015, https://kb.vmware.com/s/article/2134021.

[66] On September 13, 2017, the DHS issued a directive ordering federal departments and agencies to identify, discontinue to use, and ultimately remove the Kaspersky products from federal information systems. This directive was issued amid concerns that the Russian government and Russian intelligence agencies may use Kaspersky products to compromise federal information systems.

[67] Pamela Engel, "Why One of the World's Leading Cyber-espionage Firms Won't Touch Russia," *Business Insider*, March 19, 2015, http://www.businessinsider.com/kaspersky-and-russian-spies-2015-3.

in investigations on behalf of the Russian government and may share Kaspersky customers' data with the government.[68] Reports by *BloombergBusinessweek* from July 2017 cited internal Kaspersky emails alleging that Kaspersky personnel have accompanied Russian intelligence and police on raids and arrests.[69] A report from *The Wall Street Journal* in October 2017 shed additional light on an incident in 2015, in which hackers working for the Russian government used Kaspersky's antivirus software running on an NSA contractor's personal computer to steal details about how the United States penetrates foreign computer networks and defends against cyberattacks.[70] The U.S. government has been progressively blocking agencies from using Kaspersky. The National Defense Authorization Act for Fiscal Year 2018, signed into law in December 2017, included a ban on using "hardware, software, or services developed or provided, in whole or in part" by Kaspersky Lab, its successors, or affiliated entities.[71]

These types of business relationships can introduce risk through multiple relationships at different tiers within a single supply chain. Kaspersky's products integrate with virtual machine platforms such as Microsoft Hyper-V, Citrix XenServer, and Kernel-based Virtual Machine.[72] Kaspersky is a "VMware Integrated Partner Solutions for Networking and Security" provider, as well as one of the six partners VMware recommends for antivirus and protection solutions.[73] VMware also has a relationship with vArmour Networks, Inc., a virtual data center and cloud security company,[74] and vArmour has a partnership with Nutanix, which is itself a technology partner of Kaspersky.[75] Kaspersky antivirus products are integrated into routers, chips, and software products produced by Cisco, Juniper, D-Link, Broadcom, Amazon, and Microsoft.[76]

[68] Carol Matlack, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *BloombergBusinessweek*, March 20, 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

[69] Jordan Robertson and Michael Riley, "Kaspersky Lab Has Been Working with Russian Intelligence," *BloombergBusinessweek*, July 11, 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

[70] Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

[71] National Defense Authorization Act for Fiscal Year 2018.

[72] "Kaspersky Security for Virtualization," Kaspersky Lab, accessed October 30, 2017, http://media.kaspersky.com/en/business-security/Kaspersky%20Security%20for%20Virtualization%20Datasheet.pdf.

[73] "VMware Integrated Partner Solutions for Networking and Security," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/products/vcns/VMware-integrated-partner-solutions-networking-security.pdf; "Antivirus Best Practices for VMware Horizon View 5.x," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/techpaper/VMware-View-AntiVirusPractices-TN-EN.pdf.

[74] vArmour, "vArmour Distributed Security System Achieves VMware's Highest Level of Product Endorsement–VMware Ready," press release, September 16, 2015. https://www.varmour.com/past-press/94-varmour-distributed-security-system-achieves-VMware-s-highest-level-of-product-endorsement-VMware-ready.

[75] Keith Stewart, "It's Official: vArmour and Nutanix Team up to Deliver Simple, Secure Data Centers," vArmour blog, July 8, 2015, https://www.varmour.com/resources/blog/entry/its-official-varmour-and-nutanix-team-up-to-deliver-simple-secure-data-centers; "vArmour," Nutanix, Technology Alliances, accessed October 30, 2017, https://www.nutanix.com/partners/technology-alliance-program/varmour/; "vArmour and Nutanix Partner to Simplify and Secure Hyper-Converged, Distributed Infrastructure," *Martekwired*, July 8, 2015, https://finance.yahoo.com/news/varmour-nutanix-partner-simplify-secure-120000717.html; "Recognition," Kaspersky, Solutions, Enterprise Security, Cloud Security, accessed October 30, 2017, https://usa.kaspersky.com/enterprise-security/virtualization.

[76] Adam Mazmanian, "Kaspersky Axed from Governmentwide Contracts," *FCW*, July 12, 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx.

Chapter 4: China's Political and Economic Agenda Is Behind the Supply Chain Security Dilemma

Understanding that Chinese national political and economic policies encourage indigenous ICT manufacturing and development helps explain the risks to the U.S. ICT supply chain. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain.

PRIORITIZING INDIGENOUS ICT PRODUCTION

The Chinese government has expended significant political and economic capital in its effort to expand and indigenize its ICT production capabilities. In the 1980s, China began to rival Japan and South Korea as a producer of low-tech IT components. China's production capacity expanded throughout the 1990s, and it began to move up the value chain, producing ever more complex electronic equipment. By the late 1990s, the Chinese domestic market itself became a factor in the evolving equation. The rising incomes of China's new middle class meant that the country was now an important consumer market for the very products it had once been known for producing and exporting. Multinational tech companies shifted production and supply centers to China, launched Chinese subsidiaries, and invested in Chinese manufacturing and R&D centers to meet demand from China's rapidly growing domestic market. These deals occurred in tandem with PRC outreach to foreign multinationals, as the country encouraged foreign investment that could bring new products, technologies, and, most important, jobs to China. **Table 3** is an overview of key PRC policies enacted during this period.

Table 3
Foundational PRC Policies for Indigenous ICT Development

Date	Title	Description
1986	National High Technology Research and Development Program (863 Program)	The 863 Program funds high-technology development in strategic sectors, including IT, biology, aeronautics, automation, energy, materials, and oceanography. Government institutes, university research labs, and SOE R&D departments participate in 863 initiatives. The Chinese Academy of Sciences is the largest recipient of 863 money. In 2014, the program provided more than $5 billion for China's microchip industry, developing software to compete with Microsoft's Windows and Google Inc.'s Android, and advancing China's server manufacturing capacity. Inspur Chairman Sun Pishu is a member of China's legislature and a member of the 863 Program's expert committee. In 2014, he proposed measures to review critical technology purchases and accelerate domestic innovation efforts.
2006	National Medium- and Long-Term Plan for Science and Technology Development Plan (2006–2020)	The goal is for China to be a major center of indigenous innovation by 2020 and a global innovation leader by 2050. This plan: • Seeks to sharply reduce the country's dependence on foreign technology • Increases gross expenditures for R&D, especially for space programs, aerospace development and manufacturing, renewable energy, computer science, and life sciences • Calls for regulations in the country's government procurement law to "encourage and protect indigenous innovation," requiring a first-buy policy for major domestically made high-tech equipment and products that possess proprietary intellectual property rights, providing policy support to enterprises in procuring domestic high-tech equipment, and developing "relevant technology standards" through government procurement

Source: James McGregor, Dow Jones.[77]

[77] James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, Global Regulatory Cooperation Project, 2010), https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf; Dow Jones, "NSA Concerns Give Chinese Server Maker Inspur a Boost," *The Australian*, July 30, 2014, http://www.theaustralian.com.au/business/latest/nsa-concerns-give-chinese-server-maker-inspur-a-boost/news-story/b80feaa88eb98909ad47ea1bc11ae948.

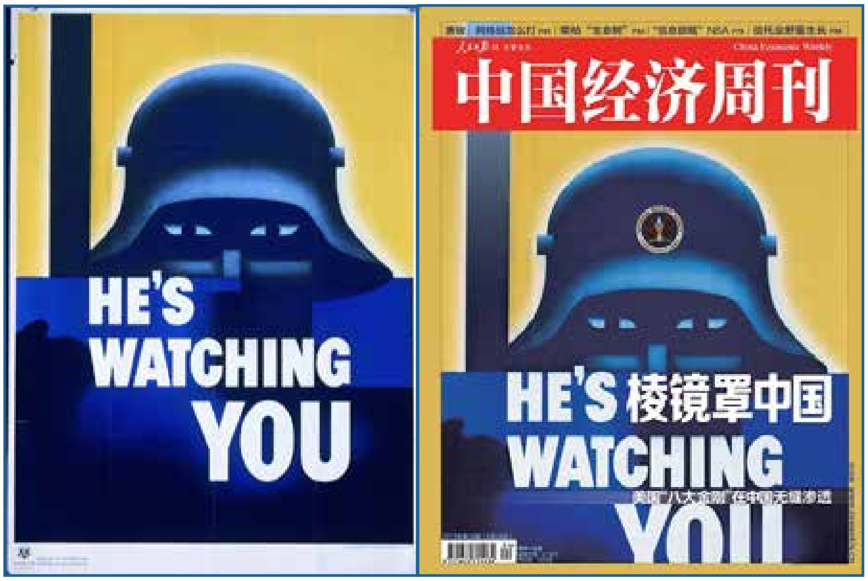
In February 2017, the PRC State Council published a press release highlighting a recent IHS Markit report indicating China has moved from being a low-cost supplier to being the center of the global supply chain.[78] As Chinese firms move up the value chain, the Chinese government has shifted the focus of its development policies. Where once the PRC government offered tax incentives and other perks to encourage foreign direct investment (FDI), the Chinese domestic market now represents a significant draw. China is less likely to offer incentives to foreign companies to do business in China and more likely to demand concessions from them in exchange for the privilege, thereby creating even more opportunities for risk insertion into the global COTS ICT supply chain.

RAISING SECURITY CONCERNS

Since 2013, the Chinese government has put pressure on U.S. ICT companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the PRC government to conduct security audits on ICT products. In the wake of Edward Snowden's 2013 allegations that the U.S. government used some of the country's technology firms to spy on foreign governments, Chinese officials began investigating Microsoft, Apple, and other U.S. technology companies.[79] Official media called for a "de-Cisco campaign" or a boycott of Cisco products.[80] In June 2013, the Chinese state-backed *China Economic Weekly* ran a cover story calling eight U.S. companies (Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm) "guardian warriors" that had "seamlessly penetrated" Chinese society.[81]

Several elements of subliminal messaging are at work here. In a move directed primarily at U.S. observers and China's educated and globalized elite, the cover of the issue that contained this article reused a U.S. World War II poster originally released to warn against German espionage.[82] **Exhibit 3** compares the two images. The image on the left is a copy of the original poster released by the U.S. Office of Emergency Management in 1942. The image on the right is the cover of *China Economic Weekly* published in June 2013, modified by the addition of the NSA insignia on the soldier's helmet.

Exhibit 3
U.S. Espionage Drives China's Nationalist IT Policy



Sources: U.S. Office of Emergency Management (1942) and *China Economic Weekly* (2013).

[78] "China Becomes Center of Global Supply Chain," State Council of the People's Republic of China, February 10, 2017, http://english.gov.cn/news/top_news/2017/02/10/content_281475564088064.htm.

[79] Eva Dou, "NSA Concerns Give Chinese Server Maker a Boost," *The Wall Street Journal*, July 29, 2014, https://www.wsj.com/articles/nsa-concerns-give-chinese-server-maker-inspur-a-boost-1406653858.

[80] Daniel H. Rosen and Beibei Bao, "Eight Guardian Warriors: PRISM and Its Implications for US Businesses in China," Rhodium Group, July 18, 2013, http://rhg.com/notes/eight-guardian-warriors-prism-and-its-implications-for-us-businesses-in-china-2.

[81] Bai Zhaoyang 白朝阳, "Meiguo 'Bada Jingang' Shentou Zhongguo Da Qi Di" 美国"八大金刚"渗透中国大起底 [United States' "Eight Guardian Warriors" Seamlessly Penetrate China], *China Economic Weekly* 中国经济周刊, June 24, 2013, http://paper.people.com.cn/zgjjzk/html/2013-06/24/content_1259857.htm.

[82] United States Office of Emergency Management, "He's Watching You" (1942), accessed from New Hampshire State Library, Unifying a Nation, https://www.nh.gov/nhsl/ww2/ww57.html.

More relevant to China’s domestic audience, the labeling of the eight U.S. tech firms as “guardian warriors” recalls the Eight-Nation Alliance that intervened militarily in China between 1899 and 1901 to suppress the Boxer Rebellion. Views on the rebellion are diverse, but in general the episode marked the flagging legitimacy of the Qing dynasty and the growing strength of anti-foreign, anti-colonialist forces in Chinese politics. Current PRC rhetoric frequently couches the Boxer Rebellion in anti-imperialist, patriotic-nationalist terms, and the Eight-Nation Alliance as a group that facilitated the collapse of the last Chinese dynasty and foreign oppression. The eight guardian warriors, then, represent not only a pernicious threat to China’s unity and independence but also a call for increased self-reliance in order to resist foreign influence. The *China Economic Weekly* article argues that while President Barack Obama made it illegal for U.S. agencies to purchase Chinese IT equipment without a federal cybersecurity investigation, no law requiring the investigation of U.S. companies yet existed in China.

In 2014, more allegations about NSA espionage efforts directed at China were reported by the German weekly *Der Spiegel* and the *New York Times*.[83] The reports alleged that in early 2009 the NSA began targeting Huawei, as well as Chinese ministries, banks, and then-president Hu Jintao. The Chinese government began to move against U.S. ICT companies soon after, launching antitrust investigations of Qualcomm and Microsoft, issuing a ban on Windows 8 on government computers, and raising concerns about the Apple iPhone’s security. In response to this pressure, Apple has promised to build an R&D center in China.[84]

EXTRACTING CONCESSIONS FROM MULTINATIONALS

The FDI Regulatory Restrictiveness Index of the Organisation for Economic Co-operation and Development (OECD) measures statutory restrictions on FDI in 62 countries, including all OECD and G20 countries, and covers 22 sectors.[85] The index gauges the restrictiveness of a country’s FDI rules by looking at the four main types of restrictions: (1) foreign equity limitations, (2) screening or approval mechanisms, (3) restrictions on the employment of foreigners as key personnel, and (4) operational restrictions such as restrictions on branching, capital repatriation, or land ownership. According to OECD data, China is the most restrictive of the G20 countries.[86]

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the United States by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. Many of these laws and policies are discussed in depth in publications by the U.S. Chamber of Commerce, the Congressional Research Service, and the U.S.-China Economic and Security Review Commission.[87] **Table 4** offers a brief overview.

[83] “NSA Spied on Chinese Government and Networking Firm,” *Der Spiegel*, March 22, 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html; David E. Sanger and Nicole Perlroth, “N.S.A. Breached Chinese Servers Seen as Security Threat,” *The New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

[84] David Barboza, “How China Built ‘iPhone City’ with Billions in Perks for Apple’s Partner,” *The New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/technology/apple-iphone-china-foxconn.html.

[85] “FDI Regulatory Restrictiveness Index,” Organisation for Economic Co-operation and Development, March 27, 2017, http://www.oecd.org/investment/fdiindex.htm.

[86] The Group of Twenty (G20) is an international forum dedicated to international cooperation on financial and economic issues. Members of the G20 include many of the world’s wealthiest nations, and collectively account for more than four-fifths of the world’s gross domestic product, three-quarters of global trade, and almost two-thirds of the world’s population.

[87] James McGregor, *China’s Drive for “Indigenous Innovation”*; Wayne M. Morrison, “China-U.S. Trade Issues,” Congressional Research Service, February 9, 2017, 35; OECD, OECD Science, Technology and Innovation Outlook 2016; Nargiza Salidjanova et al., “Economics and Trade Bulletin,” U.S.-China Economic and Security Review Commission, August 7, 2017, https://www.uscc.gov/sites/default/files/Research/August%202017%20Trade%20Bulletin.pdf; “Economics and Trade Bulletin,” U.S.-China Economic and Security Review Commission, June 2, 2017, https://www.uscc.gov/sites/default/files/trade_bulletins/June%202017%20Trade%20Bulletin.pdf.

Table 4

Chinese Laws and Policies Related to ICT and National Security

Date Issued	Title	Description
May 2015	Notice of the State Council on Issuing "Made in China 2025"	Lays out a comprehensive plan to upgrade the Chinese manufacturing sector through the use of intelligent ICT (smart manufacturing). Sets nine priority tasks over 10 sectors, with five definitive projects, including new IT, robotics, aerospace, ocean engineering, and high-end rail transportation. Calls for strengthened security reviews for investment, mergers and acquisitions, and procurement in manufacturing sectors that are related to national economy and national security.
July 2015	National Security Law	Promotes domestic and indigenous innovation in key sectors. Enables the government to conduct "national security reviews" of "foreign commercial investment, special items and technologies, Internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security."
July 2015	Guiding Opinions of the State Council on Actively Advancing "Internet+" Action	Aims to drive economic growth in China through the integration of internet technologies with manufacturing and business. Prioritizes upgrading and strengthening the security of the internet infrastructure, expanding access to the internet and related technologies, making social services more convenient and effective, and increasing both the quality and effectiveness of economic development.
January 2016	Counter-Terrorism Law	Requires telecommunications operators and internet service providers to provide technical interfaces, decryption, and other technical support assistance to public and state security organizations that are conducting activities to prevent or investigate terrorism.
July 2016	13th Five-Year Plan for Science and Technology Innovation	Aims to strengthen China's science and technology competitiveness and international influence and develop breakthroughs in core and critical technology areas in order to support economic restructuring and industrial upgrading.
November 2016	Cybersecurity Law	Restricts select data transfers out of China. Requires firms that fall under the critical information infrastructure to store their data inside China. Firms have until 2018 to comply with some data storage requirements. Requires firms that interact with the critical information infrastructure or that provide services that may affect national security to be subject to a security review by Chinese authorities. This review may be used to ensure that these services are "secure and controllable," a term used in other Chinese digital regulations, which compels foreign firms to hand over important intellectual property assets such as source code to Chinese authorities for inspection.
November 2017	Standardization Law of People's Republic of China	Revises China's 1989 Standardization Law in ways that may advantage Chinese companies over U.S. and other non-Chinese companies. During its investigation into China's practices related to intellectual property and technology transfer, the Office of the United States Trade Representative determined the standards may require U.S. companies to make product or service-related disclosures that increase costs and/or risks.

Sources: McGregor, Morrison, OECD, Salidjanova et al., U.S.-China Economic and Security Review Commission, U.S. Chamber of Commerce, Office of the U.S. Trade Representative.

The U.S. Chamber of Commerce produced reports in 2016 and 2017 detailing trade policies between the United States and China, particularly as they relate to ICT products.[88] The shift in tone over the course of a year is revealing.

[88] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT* (Washington, DC: U.S. Chamber of Commerce, 2016), https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf; U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: U.S. Chamber of Commerce, 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

The 2016 paper is cautiously optimistic that increasing trends to "deglobalize" trade could be reversed. The 2017 paper paints a darker view, seemingly more certain that China's course is increasingly set toward balkanization and creating disadvantages for foreign companies in support of domestic competitors and indigenous innovation.

These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they open themselves and federal ICT networks to Chinese cyberespionage efforts.

This threat is not theoretical. Chinese government pressure on companies to submit source code for review may occur in support of, or in tandem with, other efforts to identify vulnerabilities in U.S. ICT products. The China Information Technology Evaluation Center (CNITSEC), which conducts the security reviews of foreign companies, is run by China's Ministry of State Security. But Recorded Future, a U.S.-Swedish internet technology company focusing on cyber intelligence, has linked CNITSEC to APT3, a China-based cyberespionage unit that has hacked federal agencies and companies in the United States and Hong Kong.[89]

Microsoft has allowed the Chinese government to access its source code since 2003, when it signed an agreement with CNITSEC allowing China to participate in its Government Security Program, which grants access to the source code and technical information of several versions of Windows software.[90] In January 2010, 34 U.S. companies, including Google, Adobe, Yahoo, and Northrop Grumman, were hit by attacks from China facilitated by a previously unknown vulnerability in Microsoft's Internet Explorer. In March 2010, researchers at McAfee claimed the January attacks targeted the companies' source-code management systems in an effort to extract proprietary source code.[91]

Reports from *The Guardian* indicate that the Microsoft source code used in the attacks was obtained from Chinese IT security companies. *The Guardian*'s reporting indicates CNITSEC and its partner, Topsec, may have passed Microsoft source code to the Chinese government units that carried out the hacking.[92] Topsec's connection to the Chinese government includes work related to China's space program, its national firewall, and other high-profile state projects, such as the 2008 Olympic Games, the 2010 World Expo, and the 2010 Guangzhou Asian Games.[93]

In October 2015, IBM became the first major U.S. tech company to allow officials from China's Ministry of Industry and Information Technology to examine its proprietary source code.[94] In September 2016, Microsoft announced the opening of its new Microsoft Transparency Center in Beijing, China, which will allow government officials to analyze and test products.[95] Additional Transparency Centers are located in Belgium, Brazil, Singapore, and the United States.[96]

[89] Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Recorded Future* (blog), May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/; Mark Rockwell, "Feds Targeted in Clandestine Wolf Phishing Campaign," *FCW*, July 13, 2015, https://fcw.com/articles/2015/07/13/fed-phishing.aspx.

[90] "Microsoft and China Announce Government Security Program Agreement," Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/.

[91] Kim Zetter, "Google Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010, https://www.wired.com/2010/03/source-code-hacks/.

[92] Pascal-Emmanuel Gobry, "China Used Microsoft Source Code to Hack Google–And You?" *Business Insider*, December 7, 2010, http://www.businessinsider.com/wikileaks-china--microsoft-source-hack-google-2010-12.

[93] "Introduction to TOPSEC," Topsec, http://www.topsec.com.cn/english/about_us.html.

[94] Eva Dou, "IBM Allows Chinese Government to Review Source Code," *The Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

[95] Scott Charney, "New Beijing Transparency Center Announced," Microsoft, September 19, 2016, https://blogs.microsoft.com/on-the-issues/2016/09/19/new-beijing-transparency-center-announced/.

[96] "Government Security Program," Microsoft, June 2017, http://az370354.vo.msecnd.net/enterprise/GSP%20External%20Content%20Overview%20-%20Trust%20Center%20Version.pdf.

USING CHINESE COMPANIES TO FURTHER STATE GOALS

China is not a U.S. ally and is not likely to become one anytime soon. Moreover, the Chinese government and actors associated with it have repeatedly engaged in well-documented instances of theft and misuse of IP, as well as state-directed economic espionage. Chinese government policies summarized in **Table 4** are aimed at, among other goals, the creation and support of Chinese national champions—companies that further the government's strategic aims in return for government support.

Government support can take many forms, but it often includes preferential financing rates, preference in government contract bidding, and sometimes oligarchy or monopoly status in protected industries.[97] In the case of Chinese national champions, the support also appears to include officially sanctioned or officially conducted corporate espionage designed to improve the competitiveness of Chinese firms while potentially advancing other government interests.[98] Huawei, Zhongxing Telecommunications Corporation (ZTE), and Lenovo are three Chinese ICT companies that exhibit some of these characteristics.

Huawei is a Chinese multinational networking and telecommunications equipment company headquartered in Shenzhen.[99] Ren Zhengfei, a former officer in the People's Liberation Army (PLA) and a military technology researcher, founded Huawei in 1987 and continues to operate it.[100] Although Huawei is registered as a private company, a report by the U.S. House of Representatives Permanent Select Committee on Intelligence says Huawei:[101]

> *operates in what Beijing explicitly refers to as one of seven "strategic sectors." Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP [Chinese Communist Party] ensures that "national champions" dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.*

Huawei claims to be employee owned, but the company, unlike many Chinese corporations, has chosen not to sell shares in Hong Kong or the United States, which would require it to make financial disclosures.[102]

As early as 2000, hackers who appeared to be located in China infiltrated and exploited the networks of Nortel Networks Ltd., a foreign competitor of Huawei. Nortel was a multinational telecommunications and data networking equipment manufacturer headquartered in Canada. Nortel discovered the hacking in 2004 and determined that the hackers had obtained the passwords of seven top officials, including a previous CEO. Using China-based internet addresses, the hackers downloaded technical papers, R&D reports, and business plans, and monitored the employee email system.[103] The Nortel employee who conducted the internal investigation alleged that the hackers were based in Shanghai. Outside expert analysis determined that the rootkits installed on Nortel's systems were the work of professionals.[104]

[97] Antonio Graceffo, "China's National Champions: State Support Makes Chinese Companies Dominant," *Foreign Policy Journal*, May 15, 2017, https://www.foreignpolicyjournal.com/2017/05/15/chinas-national-champions-state-support-makes-chinese-companies-dominant/.

[98] Shane Harris, "Exclusive: Inside the FBI's Fight against Chinese Cyber-Espionage," Foreign Policy, May 27, 2014, http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/; Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, *Testimony Before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations* (July 9, 2013) (statement by Larry M. Wortzel), http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

[99] "Corporate Information," Huawei, accessed September 21, 2017, http://www.huawei.com/en/about-huawei.

[100] Michael S. Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment," *The New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

[101] Permanent Select Comm. on Intelligence, Investigative *Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, a Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence*, U.S. House of Representatives, 112th Cong. (October 8, 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

[102] Schmidt, Bradsher, and Hauser, "U.S. Panel Cites Risks in Chinese Equipment."

[103] Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach," *The Wall Street Journal*, February 14, 2012, https://www.wsj.com/articles/SB10001424052970203363504577187502201577054.

[104] Jameson Berkow, "Nortel Hacked to Pieces," *Financial Post*, February 25, 2012, http://business.financialpost.com/technology/nortel-hacked-to-pieces.

Nortel changed the compromised passwords, but six months later the hackers appeared to retain some access to the company's systems. Every month or so, a few computers on Nortel's network would send small bursts of data to one of the internet addresses in Shanghai involved in the password-hacking episodes. Subsequent investigations revealed that the hackers had installed spyware on Nortel's computers, could control some computers remotely, and had set up an encrypted communication channel to an internet address near Beijing. Nortel filed for bankruptcy in 2009. The hacking incident was not fully disclosed when the company began selling off assets, and reports from former Nortel employees indicate that firms such as Avaya, which acquired Nortel assets following the bankruptcy, may have inadvertently purchased compromised Nortel IT equipment, leaving Avaya's systems vulnerable to infiltration by the same hackers who targeted Nortel.[105] Unconfirmed reports suggest that the hackers who targeted Nortel (as well as Motorola and Cisco during the same period) were working on behalf of Huawei, which had surpassed its U.S. competitor, Cisco, in several core markets.[106]

Huawei has been the subject of numerous investigations and congressional hearings regarding the company's alleged ties to the Chinese Communist Party and the PLA.[107] In February 2011, the Committee on Foreign Investment in the United States issued a recommendation that Huawei voluntarily divest the assets it received in a 2010 deal with 3Leaf, a U.S. company that developed advanced computer technologies. In response, Huawei published an open letter to the U.S. government denying the existence of security issues in the company or its equipment and requesting a full investigation into its corporate operations.[108] The House Permanent Select Committee on Intelligence initiated an investigation into Huawei and ZTE in November 2011 and produced a report in October 2012. The following were among the report's recommendations:

- *U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment from their systems.*

- *Private sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence, and thus pose a security threat to the United States and to our systems.*[109]

Congressional concern with Huawei and ZTE has continued. In January 2018, U.S. Representative Mike Conaway (R-TX) introduced the Defending U.S. Government Communications Act, which would prohibit the U.S. government from purchasing and using "telecommunications equipment and/or services" from Huawei and ZTE.[110]

Huawei and ZTE are not the only Chinese companies to be accused of such activity. The Chinese computer and server manufacturer Lenovo is a similar case. Lenovo originally formed in 1984 as the New Technology Development Company, a component of the state-run Chinese Academy of Sciences Institute of Computing Technology.[111] The founder of Lenovo was educated at the Xi'an Military Communications Engineering Institution of the PLA, now Xidian University. The university has close connections with the PLA and is considered to be a link between China's civilian and military research on cybersecurity.[112] Additionally, Lenovo's CEO, who succeeded its

[105] Tom Warren, "Hackers Roamed Nortel's Network for Years without Detection," *The Verge*, February 14, 2012, https://www.theverge.com/2012/2/14/2797047/nortel-undetected-hacking-breach.

[106] Mark Anderson, "The Sony Hack and Nortel's Demise: Piracy vs. Crown Jewel Theft," *Forbes*, January 21, 2015, https://www.forbes.com/sites/valleyvoices/2015/01/21/the-sony-hack-and-nortels-demise-piracy-vs-crown-jewel-theft/#1efa1d54f0c9.

[107] *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

[108] Ken Hu, "Huawei Open Letter," *The Wall Street Journal*, February 5, 2011, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

[109] *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

[110] Defending U.S. Government Communications Act, H.R. 34747, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/4747; Andrew Liptak, "A New Bill Would Ban the US Government from Using Huawei and ZTE Phones," *The Verge*, January 14, 2018, https://www.theverge.com/2018/1/14/16890110/new-bill-ban-huawei-zte-phones-tech-congress-mike-conaway-cybersecurity.

[111] Nathaniel Ahrens and Yu *Zhou, China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan, CASE STUDY: Lenovo* (Washington, DC: Center for Strategic and International Studies, January 2013), https://www.csis.org/analysis/china%E2%80%99s-competitiveness-lenovo.

[112] Edward Wong, "University in Xi'an Opens School of Cyberengineering," *Sinosphere: Dispatches from China* (blog), *The New York Times*, January 6, 2015, https://sinosphere.blogs.nytimes.com/2015/01/06/university-in-xian-opens-school-of-cyberengineering/.

founder, was educated at China's University of Science and Technology, which was established and resourced by the CAS.[113] The CAS and its individual members have a history of coordinating with the Chinese military, including its cyber and electronic warfare operations.[114] The Chinese government, through Legend Holdings Limited, is the largest shareholder of Lenovo stock. As of June 2017, the CAS (through CAS Holdings) owned 34.83 percent of Legend and was identified as Legend's controlling shareholder.[115] In 2017, Legend had 31.48 percent ownership in Lenovo.[116] Legend, which was formed by Lenovo's founder, operates as the external investment vehicle and asset management unit of the CAS.[117] Lenovo's growth has been attributed to the economic and political support it receives from the Chinese government, including the use of state-owned intellectual property resources.[118]

Lenovo has been linked to Chinese state-led cyberespionage efforts. Lenovo products have been banned by intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States (Five Eyes Countries) since the mid-2000s, when laboratories of the British intelligence agencies Military Intelligence, Section 5 and Government Communications Headquarters discovered "backdoors"[119] and vulnerable firmware in Lenovo products.[120] In 2006, after congressional inquiries into the purchase of 16,000 Lenovo computers, the U.S. Department of State said the purchased computers would be used only on unclassified systems.[121] In 2015, the U.S. Navy announced it would replace servers for its guided missile cruisers and destroyers after Lenovo acquired certain IBM server and software product lines, due to concerns that the equipment could be compromised during maintenance or remotely accessed by the Chinese government.[122] In 2016, several incidents suggested the DoD may have banned Lenovo products owing to concerns about cyber spying against Pentagon networks and concerns that the company is installing backdoors in its products for the purposes of espionage. In April 2016, an Air Force email appeared to order that Lenovo products be removed from DoD networks. This message was subsequently retracted by Air Force and Pentagon spokeswomen.[123] In October 2016, *The Washington Free Beacon* reported that the Pentagon's Joint Staff had produced an internal report warning against using Lenovo equipment.[124]

In addition, Lenovo is believed to have been complicit in installing Superfish spyware and potentially a BIOS backdoor on a number of its computer products.[125] Superfish is a preloaded software shipped with Lenovo computers that ostensibly monitored internet browser traffic to improve advertisements, but also allowed hackers to read all encrypted browser traffic, including banking transactions, passwords, emails, and instant messages. The DHS U.S.

[113] "USTC Introduction," University of Science and Technology of China, About, October 14, 2016, http://en.ustc.edu.cn/about/201101/t20110113_87798.html.

[114] John Costello, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Intelligence Agencies: Reform and Future," June 9, 2016, http://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony060916.pdf.

[115] Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report" (Hong Kong Stock Exchange, September 14, 2017), 45, http://www.hkexnews.hk/listedco/listconews/SEHK/2017/0929/LTN201709291285.pdf.

[116] Factiva Database, Dow Jones and Reuters, New York.

[117] Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report," 30; Factiva Database, Dow Jones and Reuters, New York.

[118] Ahrens and Zhou, *China's Competitiveness*.

[119] A backdoor is a means of bypassing normal authentication or encryption in a computer system, product, or embedded device. A backdoor may be a hidden part of a program, a separate program, or code in the firmware of hardware or parts of an operating system.

[120] Adi Robertson, "Lenovo Reportedly Banned by MI6, CIA, and Other Spy Agencies over Fear of Chinese Hacking (Update)," *The Verge*, July 30, 2013, https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears; Christopher Joye, Paul Smith, and John Kerin, "Spy Agencies Ban Lenovo PCs on Security Concerns," *Financial Review*, July 27, 2013, accessed via WayBackMachine, https://web.archive.org/web/20130729011053/http://www.afr.com/p/technology/spy_agencies_ban_lenovo_pcs_on_security_HVgcKTHp4bIA4ulCPqC7SL; Cahal Milmo, "MI6 and MI5 'Refuse to Use Lenovo Computers' over Claims Chinese Company Makes Them Vulnerable to Hacking," *Independent*, July 29, 2013, http://www.independent.co.uk/news/uk/home-news/mi6-and-mi5-refuse-to-use-lenovo-computers-over-claims-chinese-company-makes-them-vulnerable-to-8737072.html.

[121] "US Government Restricts China PCs," *BBC News*, May 19, 2006, http://news.bbc.co.uk/2/hi/americas/4997288.stm.

[122] Phil Muncaster, "US Navy Looks to Dump Lenovo Servers on Security Concerns—Report," I*nfosecurity Magazine*, May 7, 2015, https://www.infosecurity-magazine.com/news/us-navy-dumps-lenovo-servers/; Megan Eckstein, "Navy Needs New Servers for Aegis Cruisers and Destroyers after Chinese Purchase of IBM Line," *USNI News*, May 5, 2015, https://news.usni.org/2015/05/05/navy-needs-new-servers-for-aegis-cruisers-and-destroyers-after-chinese-purchase-of-ibm-line.

[123] Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," *The Washington Post*, April 22, 2016, https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html.

[124] Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," *The Washington Free Beacon*, October 24, 2016, http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/.

[125] Vijay, "Lenovo PCs and Laptops Seem to Have a BIOS Level Backdoor," *TechWorm*, August 12, 2015, http://www.techworm.net/2015/08/lenovo-pcs-and-laptops-seem-to-have-a-bios-level-backdoor.html.

Computer Emergency Readiness Team issued an alert and mitigation details in response.[126] Users later discovered that Lenovo computers shipped with a rootkit-style covert installer that would reinstall unwanted software on computers after users had deleted it. In September 2017, Lenovo reached a settlement with the Federal Trade Commission over charges that the company harmed consumers. As part of the settlement, Lenovo is required to implement a comprehensive software security program for consumer software.[127] The security program will be subject to third-party audits.

TARGETING U.S. GOVERNMENT CONTRACTORS

The Chinese government and Chinese nationals have previously been linked to attempts to illegally obtain source code from U.S. ICT companies. Chinese actors, including those connected to the government, have a history of trying to obtain sensitive information about U.S. companies in order to exploit their networks, replicate their technologies, and outcompete them in the global marketplace. China-linked hacking has repeatedly targeted U.S. federal government entities and U.S. federal government contractors, including many key players in ICT contracting.[128]

In 2007, the FBI investigated Unisys after a dozen DHS computers that Unisys was supporting were compromised and significant amounts of unclassified but sensitive information was transferred to Chinese websites. It remains unknown precisely what information was removed.[129] In 2013, Bloomberg reported on China-linked hacking dating back to 2007 that targeted the North American arm of QinetiQ, a British satellite, drone, and software defense manufacturer.[130] QinetiQ supplies spy satellites, bomb disposal robots, and other products to the U.S. military. Through compromised QinetiQ networks, the hackers targeted the networks of NASA, U.S. rifle divisions, cybersecurity divisions, and databases related to the U.S. Army's Apache and Blackhawk helicopter fleet. According to *Bloomberg*, investigators attributed the attack to a group of Shanghai-based hackers nicknamed the "Comment Crew," a group linked by the cybersecurity firm Mandiant to PLA Unit 61398.[131]

China-linked hackers have also targeted RSA Security, a network security company that is a subsidiary of Dell. RSA's SecurID system is widely used by the U.S. government and its contractors for log-in security.[132] The most recent breach appears to have occurred in 2011, when a cyberattack on RSA Security led to data loss associated with RSA's SecurID system. In 2012, Gen. Keith Alexander, then director of the NSA and the head of U.S. Cyber Command, indicated in testimony before the Senate Armed Services Committee that RSA was a victim

[126] Department of Homeland Security, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing," February 20, 2015, https://www.us-cert.gov/ncas/alerts/TA15-051A.

[127] Federal Trade Commission, "Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops That Compromised Online Security," September 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

[128] Hanqing Chen, "A Recent History of China's Cyber Attacks on the United States," *Pacific Standard*, September 4, 2014, https://psmag.com/environment/chinas-cyber-attacks-united-states-89919; "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html; Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

[129] Mike Masnick, "FBI Investigating Unisys for Not Preventing US Gov't Computers from Getting Hacked," *Techdirt*, September 25, 2007, https://www.techdirt.com/articles/20070924/135824.shtml; Jason Mick, "Unisys Blamed for China-Connected Homeland Security Hacks," *DailyTech*, September 26, 2007, http://www.dailytech.com/Unisys+Blamed+for+ChinaConnected+Homeland+Security+Hacks/article9043.htm; Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html; "Investigators: Homeland Security Computers Hacked," CNN, September 24, 2007, http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html.

[130] Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg, May 2, 2013, https://www.bloomberg.com/news/articles/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets; Michael Riley and Alex Tribou, "Hackers in China Compromise U.S. Defense Secrets," Bloomberg, May 2, 2013, https://www.bloomberg.com/graphics/infographics/hackers-in-china-compromise-us-defense-secrets.html.

[131] "APT1: Exposing One of China's Cyber Espionage Units," Mandiant.

[132] Elinor Mills, "China Linked to New Breaches Tied to RSA," CNet, June 6, 2011, https://www.cnet.com/news/china-linked-to-new-breaches-tied-to-rsa/.

of Chinese cyberespionage.[133] According to 2013 testimony by the executive chairman of RSA, the company detected a targeted cyberattack on its systems and recognized that product information had been extracted. RSA publicly disclosed the breach and alerted customers to help them mitigate the effects. The company took its own remediation steps, including replacing nearly all of the 40 million SecurID tokens in use.[134] Industry press reports indicate that RSA's reluctance to publicly disclose which data had been stolen during the breach may have led to breaches at other defense contractors, including Lockheed Martin, L-3 Communications, and Northrop Grumman.[135] In June 2011, Lockheed Martin confirmed that the breach it experienced was due to data stolen from RSA.[136]

In July 2013, researchers from Dell's SecureWorks unit identified hackers targeting an unnamed maker of audio-visual conference equipment.[137] The Dell researchers linked the hackers to the Chinese hacking group that breached RSA Security in 2011. Dell's researchers speculated the hackers were attempting to obtain source code of the company's products in order tap into boardroom and other high-level remote meetings. In December 2015, a former software engineer for IBM in China was arrested and charged with economic espionage and theft of trade secrets.[138] The engineer had stolen source code related to IBM's proprietary clustered file system, which facilitates faster computer performance, and attempted to share it with the PRC's National Health and Family Planning Commission.[139]

[133] Kelly Jackson Higgins, "China Hacked RSA, U.S. Official Says," *Dark Reading*, March 29, 2012, https://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409; *Hearing on U.S. Strategic Command and U.S. Cyber Command, Testimony Before the Senate Armed Services* (March 27, 2012) (statement of Keith B. Alexander), 13, https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%203-27-12.pdf.

[134] Arthur W. Coviello, Jr., "Written Testimony before the U.S. Senate Committee on Commerce, Science & Transportation," June 25, 2013, https://www.emc.com/collateral/corporation/coviello-congressional-testimony-2013.pdf; Peter Bright, "RSA Finally Comes Clean: SecurID Is Compromised," *Ars Technica*, June 6, 2011, https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised/.

[135] Elinor Mills, "Attack on RSA Used Zero-day Flash Exploit in Excel," CNet, April 5, 2011, https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/; "Frequently Asked Questions about RSA SecurID: Information for RSA Customers," EMC, 2011, https://www.emc.com/collateral/guide/11455-customer-faq.pdf.

[136] Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times*, June 3, 2011, http://www.nytimes.com/2011/06/04/technology/04security.html.

[137] Joseph Menn, "Chinese Hackers Target Remote Conferencing Gear: Dell Researchers," Reuters, July 31, 2013, https://www.reuters.com/article/us-china-hacking/chinese-hackers-target-remote-conferencing-gear-dell-researchers-idUSBRE96U0YI20130731.

[138] Nate Raymond, "Ex-IBM Employee from China Arrested in U.S. for Code Theft," Reuters, December 8, 2015, https://www.reuters.com/article/ibm-crime-china/ex-ibm-employee-from-china-arrested-in-u-s-for-code-theft-idUSL1N13X2LD20151208.

[139] "Chinese National Charged for Stealing Source Code from Former Employer with Intent to Benefit Chinese Government," Department of Justice, June 14, 2016, https://www.justice.gov/opa/pr/chinese-national-charged-stealing-source-code-former-employer-intent-benefit-chinese.

Chapter 5: Closing Loopholes: Recommended SCRM Actions

Federal SCRM efforts have yet to be fully developed, and gaps in resources and processes continue to exist that allow procurement of high-risk technologies, or deployment of moderate- to low-risk technologies in ways that fail to mitigate supply chain risk. Given the budgetary challenges many federal agencies face, decisions are made on the basis of reducing cost in a way that inadvertently increases risk. Several paths could be taken to improve federal ICT supply chain security. Some involve legislative action, while others leverage federal acquisition authority.

The sections below describe four paths that should be evaluated as solutions to enhance federal ICT supply chain security, where a comprehensive solution will potentially implement more than one recommendation. Establishing a centralized leadership for SCRM, expanding legislative provisions related to SCRM, and promoting supply chain transparency are the most effective ways of improving federal ICT supply chain security, align with how industry thinks and functions, and will likely provide greater benefit and more public and private sector adoption than modifications to the role of NIST or other federal trade regulations.

ESTABLISHING CENTRALIZED LEADERSHIP FOR SCRM

Congress or the Executive Branch should (1) name the organization(s) charged with SCRM leadership, (2) provide specific resources for SCRM, and (3) encourage information sharing and consolidation of federal SCRM efforts. In the current SCRM ecosystem, responsibility for risk management is held at different levels within agencies, resulting in SCRM offices and efforts, such as those at NASA and the Departments of Energy, Commerce, and Defense, that function largely as under-resourced stovepipes, often lacking executive sponsorship or oversight, and catering to the needs and procurement policies of individual clients. Entities such as the DoD and the intelligence community maintain largely separate policies, many of which are not transparent or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons. Additionally, these programs may be concerned with initial acquisition, rather than system lifecycle concerns.

Although the nature of commercial ICT means that the universe of potential suppliers serving the federal government is extremely large, SCRM analysis conducted at the GSA, Department of Energy, NASA, and Department of Commerce often covers the same set of ICT suppliers for different federal government clients. This duplication of effort is wasteful and unnecessary, and negatively affects U.S. national security posture through misspent resources and inconsistent activities. Congress or the Executive Branch could establish centralized leadership, as well as a function, to carry out baseline SCRM analysis for the entire federal government, freeing individual agencies to focus on unique suppliers and technologies and how the identified risks impact their programs. This entity would have to be resourced and staffed appropriately, and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering federal ICT networks.

The OMB should assign this authority—through modifications to Circular A-130—to the GSA, the DHS, or another federal agency that is often tasked with shared services. The GSA, which is already responsible for vetting and managing the federal government's relationship with more than 30,000 suppliers, would be a logical center of action for this effort. Given its government-wide procurement and acquisition mission, the GSA is capable of deciding what categories of risk this baseline level of analysis should include and what level of detail the analysis should pursue. It would be wise to cast as wide a net as possible, including both technical and security risks, as well as market and business risks. Funding such a venture to the point where it could create comprehensive and authoritative information would reduce the burden for agency-specific SCRM and enable agencies to build from the same foundation, focusing their efforts on particular configurations and implementation situations. Funding for this entity could include seed money as well as a cost-reimbursable model with the collaborating agencies.

However, basing a centralized SCRM effort in the GSA could present challenges. The GSA's mission is negotiating the best deal for the federal government in any procurement. Additionally, the GSA often contracts with value-added resellers such as Mythics, DLT Solutions, Immix Group, Carahsoft, and CDW-G rather than with original equipment manufacturers (OEMs). There have been instances of OEMs (e.g., Oracle in September 2016) abandoning the GSA Schedule Contracts[140] because the effort to secure and maintain the contracts outweighed the benefits.[141] Dealing with value-added resellers rather than OEMs introduces additional risk into the federal ICT supply chain. Patrick Finn, a former senior vice president for Cisco, told Federal News Radio, "It's not uncommon for an OEM to be contacted by disgruntled customers who procured through GSA only to find out that the product was gray market or, worse, counterfeit."[142] Thus, placing SCRM for federal ICT in the hands of the GSA or any other federal agency could require not only financial and policy shifts but also cultural ones for both the government and industry. Financial cost is an element of SCRM analysis, but it should be weighed in context with security considerations.

Sharing SCRM information across the government must be done in an effective and transparent manner. The Department of Veterans Affairs (VA) has created the publicly accessible One-VA Technical Reference Module (TRM), which provides detailed information on technical risk assessments conducted by the One-VA TRM team, along with public decisions about the VA's investment or divestment in certain technologies. The TRM includes a public access site that provides TRM content, a VA internal access site that allows users to make inquiries and request technology assessments, and a TRM team collaboration site, which allows content authoring and Wiki-based development that can be pushed to published sites.[143] Users of the TRM can see when a technology was last assessed, what findings were recorded, and what actions and policies VA leadership has recommended in response to the TRM team's findings. Using a similar portal for SCRM, with distinct levels of public and government-only access, would be valuable to all federal SCRM efforts; it would prevent duplication of effort, save time, and enable agency-specific assessments to build from a common foundation and share their risk mitigation strategies. Additionally, by leveraging technology the government-wide sharing would be able to scale and sustain a robust program for all collaborating agencies.

EXPANDING THE WOLF PROVISION

Congress should expand legislative actions that address risk linked to the nature of an ICT manufacturer as well as the manufacturer's location. The Wolf Provision, or Section 516 (subsequently 515) of the 2013 Consolidated and Further Continuing Appropriations Act, is one example. This provision was added by then U.S. Representative Frank Wolf (R-VA), who chaired the House subcommittee that oversees the Departments of Commerce and Justice, NASA, and the National Science Foundation. Initially introduced in 2013, Section 516 prevented the Departments of Commerce and Justice, NASA, and the National Science Foundation from acquiring IT without first conducting a risk assessment. If the IT system was "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China" and the federal entity still wished to purchase it, then the entity had to explain to Congress why the acquisition was in the national interest of the United States.[144]

Although the Wolf Provision was criticized by industry and considered too specifically anti-China, the language of the original provision acknowledged that subjecting products to additional scrutiny purely on the basis of geographic location is not an effective course of action, especially when it comes to global ICT supply chains. The original call for scrutiny of products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by the People's Republic of China," makes clear that the potential for risk does not depend solely on the manufacturing or assembly location of a product but rather on the nature of the entity overseeing production. The language of the provision was modified in 2014, and the current provision (now in Section 515 of the Appropriations Act) no longer specifically mentions China. Instead, it includes language drawn from the NIST publication FIPS 199, which requires risk assessments for high-impact or moderate-impact information

[140] GSA Schedule Contracts, also known as GSA Schedules or Federal Supply Schedules, are indefinite delivery, indefinite quantity, long-term contracts under the GSA's Multiple Award Schedule Program.

[141] Jason Miller, "Oracle to Leave GSA Schedule: A Signal of Broader Change?" *Federal News Radio*, September 26, 2016, https://federalnewsradio.com/reporters-notebook-jason-miller/2016/09/oracle-leave-gsa-schedule-signal-broader-change/.

[142] Miller, "Oracle to Leave GSA Schedule."

[143] Paul Tibbits, "DoD-VA Collaboration to Develop a Single Electronic Health Record: SOA as a Design Pattern," July 14, 2011, http://www.omg.org/news/meetings/workshops/SOA-HC/presentations-2011/14_FS-1_Tibbits.pdf.

[144] Consolidated and Further Continuing Appropriations Act, 2013, H.R. 933, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/933/text.

systems. The current provision still applies only to the Departments of Commerce and Justice, NASA, and the National Science Foundation.[145]

Currently, no federal entities have all-encompassing risk assessment programs, nor are they directed to do so or be held accountable. The programs that do exist are not adequately resourced for effective implementation, and the fact that each agency interprets the requirements for itself means that SCRM practices can vary within—and between—federal agencies. Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. Another is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present information about (1) their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks.

Another option is to modify the language in the Wolf Provision to direct extra scrutiny at products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by" nation states or entities known to pose a potential supply chain or intelligence threat to the United States. These nation states or entities could include members of the existing Sensitive Foreign Nations Control List, the Office of the United States Trade Representative's Special 301 Report Priority Watch List, or some appropriate combination of the two.[146] This type of language would direct appropriate scrutiny at products produced by entities linked to the Chinese government, but would not place significant burden on ICT suppliers sourcing from other suppliers that may have some production facilities in China.

PROMOTING SUPPLY CHAIN TRANSPARENCY

Congress should encourage transparency and accountability for supply chains. Although this report addresses supply chains that intersect China, those are not the only sources of risk. The sheer magnitude of China's influence as a supplier and manufacturer, combined with sometimes undisclosed links between the Chinese government and Chinese firms, creates risk in federal ICT procurement. Requiring federal ICT suppliers to publish or make available information on their supply chain would increase the ability of the federal government to source responsibly and securely, and to respond to breaches in an efficient manner. The federal acquisition community could also be required to build supply chain transparency requirements or disclosures into ICT procurements for first- and second-tier suppliers, and then require that sub-tiers have this included in their flow-down clauses. Rather than seeking supply chain information from a company after an incident, the federal government and its industry partners would already have that information on hand. This information would allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers.

In testimony before the House Subcommittee on Communications and Technology in May 2013, Mark L. Goldstein, GAO director of physical infrastructure issues, reviewed findings from a GAO report regarding measures the governments of Australia, India, and the United Kingdom take to secure their ICT infrastructures.[147] India's licensing requirements include explicit supply chain measures such as requiring telecommunications service providers to keep a record of the supply chain for their hardware and software, and requiring suppliers to allow providers or government entities to inspect the supply chain. In the event of a security breach or an act of intentional omission, the Indian government can cancel the license of the provider and blacklist the vendor that supplied the

[145] Consolidated Appropriations Act, 2017, H.R. 244, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/244/text.

[146] "Attachment G Sensitive Foreign Nations Control," Department of Energy, 2014, https://energy.gov/sites/prod/files/2014/08/f18/alliance_partvII-g.pdf; Office of the United States Trade Representative, 2017 Special 301 Report (Washington, DC: Office of the United States Trade Representative, 2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

[147] *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment, Testimony Before the House Subcommittee on Communications and Technology, Committee on Energy and Commerce* (May 21, 2013) (statement by Mark L. Goldstein), https://www.gao.gov/assets/660/654763.pdf.

hardware or software that caused the security breach.[148] This policy is similar to Section 806 authorities incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) as a final rule in October 2015.[149] Pursuing similar policies, or requiring federal contractors to provide supply chain information as part of federal contract requirements, would provide an additional layer of SCRM security when the program requires this level of rigor.

Dodd-Frank Limitations Are Future SCRM Lessons

There are challenges in significantly improving supply chain transparency, and important lessons can be learned from the experience of Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which aimed to reduce violence in the Democratic Republic of the Congo by limiting U.S. procurement from actors fueling conflict in the DRC. In addition to other consumer protection provisions, Section 1502 and the ensuing Securities and Exchange Commission (SEC) rules require some companies to document the use in their products of "conflict minerals" through SEC Specialized Disclosure (SD) filings and Conflict Mineral Reports.[150]

The corporate responsibility supplier lists issued by HP, Dell, and Microsoft provide information on the first tier of the federal ICT supply chain, but the SD filings and Conflict Mineral Reports provide information on the deepest tier, the ultimate source point of the raw material a vendor is using for its ICT products. Since the passage of Dodd-Frank Section 1502 and the publication of related SEC rules, companies have filed four rounds of SD filings with the SEC and reportedly invested four years in further investigating and performing due diligence on their supply chains. And yet failings and inconsistencies remain, highlighting the scope of the challenge.

The transparency introduced by Section 1502 and the SEC rules has forced companies to diligently investigate their own suppliers, many for the first time. The policy has also raised awareness of what responsible supply chain management and responsible sourcing entail. Early on, some companies chose not to source from central Africa as a way of avoiding conflict minerals, failing to realize that global supply chains mean that conflict minerals can end up in smelters in Belgium, China, Morocco, or the United Arab Emirates. This has clear parallels to global ICT supply chains, where components may pass through several countries before being incorporated into a final product.

As Dodd-Frank made clear, the threat to U.S. national security was not minerals sourced from the DRC and adjoining countries, but rather minerals sourced from mines controlled by parties to the DRC conflict. To scope this outward, the supply chain threat to U.S. national security is not merely from products manufactured in China, or even products manufactured by Chinese businesses, but rather from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by nation states or entities known to pose a potential supply chain or intelligence threat to the United States, of which China is one.

Recommendations for improving supply chain transparency with respect to conflict minerals are applicable to supply chain transparency more generally.[151] When scoped out to ICT supply chains, new reporting requirements could require companies to note the location of their suppliers' manufacturing centers, and to identify which manufacturing centers are located in nation states known to pose a potential supply chain or intelligence threat to the United States. If a company cannot identify its suppliers' manufacturing locations, or if the location it reports appear inaccurate, it could be a warning sign that their SCRM program is not sufficient to protect the security concerns of the U.S. government.

[148] *Telecommunications Networks* (Goldstein).

[149] Susan Borschel, "New Department of Defense Requirements Relating to Supply Chain Risk," *Government Contracting Insights*, November 13, 2015, http://govcon.mofo.com/national-security/new-department-of-defense-requirements-supply-chain-risk/.

[150] Conflict minerals are defined by U.S. legislation and SEC rules as the four metals tantalum, tin, tungsten, and gold. Tantalum, tin, and tungsten are the derivatives of the minerals columbite-tantalite (coltan), cassiterite, and wolframite, respectively. Many of these metals are sourced from the Democratic Republic of the Congo or adjoining countries. The most common conflict minerals are casserite (tin), coltan (tantalum), wolframite (tungsten), and gold, which are often collectively termed "3TG."

[151] Jeff Schwartz, "The Conflict Minerals Experiment," *Harvard Business Law Review 6* (January 2015), https://ssrn.com/abstract=2548267 or http://dx.doi.org/10.2139/ssrn.2548267; *Testimony Before the House Subcommittee on Monetary Policy and Trade, Committee on Financial Services* (November 17, 2015) (statement by Jeff Schwartz), https://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-jschwartz-20151117.pdf.

UTILIZING FEDERAL ACQUISITION AUTHORITIES

The final recommendation to enhance SCRM is to use the purchasing power of the U.S. government to require commercial suppliers to meet certain cybersecurity and SCRM standards to be eligible for federal contracts.[152] This option would make SCRM issues a priority for all industry partners interested in competing for government contracts, raising their level of security before they even have access to sensitive federal information. Increasing the security posture of entities before they become a target could help them defend themselves, and the federal government, against attacks from actors linked to China.

Federal contracts could use acquisition methods, including contract clauses and flow-down requirements, to require contractors and subcontractors to meet such standards. The federal government must be clear about the risk concerns and thresholds so that industry can clearly understand, based on each program, where to include SCRM investments. Although a minimum level of SCRM should be documented, not every procurement will identically use a product or service. A strict and inflexible requirement for every acquisition and supplier to undergo the maximum level of SCRM activities will be costly and unworkable.

One example of this approach is DFARS regulations on unclassified controlled technical information and controlled unclassified information, categories of information that are considered sensitive but are not classified and regulated by the federal government. These regulations require contractors to implement specific security measures in accordance with NIST SP 800-171, including access control, training, system audit records to monitor system activity, media protection and disposal, and other requirements. These measures are a necessary step, but may not mitigate the risk posed by ICT components produced in China or by entities linked to the Chinese government. NIST SP 800-171 took effect on December 13, 2017, for the DoD, the GSA, and NASA.[153]

Meanwhile, through their joint authority, the DoD, the GSA, and NASA are proposing a similar Federal Acquisition Regulation clause for contractors that handle, possess, use, share, or receive controlled unclassified information for other federal agencies.[154] This rule would have a similar effect as the DFARS and is an example of another way NIST recommendations can become obligatory.

[152] Robert S. Metzger, "Threats to the Supply Chain: Extending Federal Cybersecurity Safeguards to the Commercial Sector," Bloomberg Law, June 8, 2015, https://www.bna.com/threats-supply-chain-n17179927448.

[153] Matt Kozloski, "Everything You Need to Know about NIST 800-171," Kelser, December 16, 2016, https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171.

[154] Undersecretary of Defense for Acquisition, Tech. and Logistics, "Open FAR Cases as of 10/31/2017," Department of Defense, accessed October 31, 2017, http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf; "Federal Acquisition Regulation (FAR); FAR Case 2017-016, Controlled Unclassified Information (CUI)," Office of Information and Regulatory Affairs, Office of Management and Budget, accessed October 31, 2017, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN56.

Chapter 6: Future Considerations

As stated at the beginning of this report, the attacks on U.S. federal ICT networks will only grow as the attack vectors—and the speed with which they can be reached—increase.

As the U.S. government develops enhanced SCRM policies and regulations, it is imperative to understand—and have a strategy to address—the risk developing technologies may pose to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. With China's focus on proactive measures, the United States should adopt the same forward-leaning posture focused on security.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within in it. In 2016, researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of computer monitors.[155] In 2017, researchers uncovered vulnerabilities in HP, Dell, and Lexmark printers that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[156] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly downloaded the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[157] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[158] The federal government's ability to identify risks, to protect federal information systems, and to respond to and recover from attacks and breaches hinges on developing a comprehensive understanding of the supply chain risk.

Other aspects of supply chain risk depend on technologies that are not yet developed or deployed, such as 5G mobile network technology, which is expected to start deploying in 2020. 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of the Internet of Things.[159] The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round-trip delay (latency[160]) to under one millisecond.[161] Although the finalization of 5G

[155] Franceschi-Bicchierai, "Hackers Could Break into Your Monitor."

[156] Tom Spring, "Flaws Found in Popular Printer Models," *Threat Post*, January 31, 2017, https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

[157] Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017, https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

[158] India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017, http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25, 2017, https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017, https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

[159] Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," Data Center Dynamics, October 7, 2016, http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

[160] Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

[161] Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," TechRepublic, https://www.techrepublic.com/article/does-the-world-really-need-5g/.

standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, so China could emerge as an industry leader in this technology.[162]

In 2016, the United States ranked first in patent filings for the 39th year in a row.[163] However, China's efforts to expand its ownership of IP are increasing; if this trend continues, China could overtake the United States in two years as the largest user of the international Patent Cooperation Treaty system. According to data from the World Intellectual Property Organization, Huawei and ZTE (along with Qualcomm) have been the top three patent filers each year since 2012.[164]

It is difficult to use patent and other IP data as a measure of a country's innovation because of differences in the policies of national patent offices and the inherent challenge of weighing the influence of any one IP application. It is also difficult to ascertain in advance which IP claims are essential to standards and which will win out when subjected to litigation. The Center for International and Strategic Studies argues that context is necessary when using patents to measure China's innovation.[165] The National Patent Development Strategy of China's State Intellectual Property Office explicitly equates patent generation with innovation. To encourage companies to file patents, the Chinese government offers incentives such as cash bonuses, subsidies, and lower corporate income taxes. This strategy might encourage quantity over quality, so that some State Intellectual Property Office patents are awarded for incremental innovations and design modifications rather than dramatic innovations.

Moreover, large increases in domestic patent filings in China have not translated into large increases in the number of triadic patents, which are patents filed jointly in the three largest global technology markets: the Japanese Patent Office, the U.S. Patent and Trade Office, and the European Patent Office. The Center for International and Strategic Studies notes, "While China now processes the greatest number of domestic patent applications annually, these patents do not hold up under the more stringent requirements of the international patent system."[166] Additionally, Chinese patent applications are not spread widely among Chinese firms but rather are concentrated in the hands of government-backed ICT firms such as Huawei and ZTE.

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[167] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[168] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[169]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[170] **Exhibit 4** shows share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for

[162] Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017, https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.

[163] World Intellectual Property Organization, "Record Year for International Patent Applications in 2016; Strong Demand Also for Trademark and Industrial Design Protection," press release, March 15, 2017, http://www.wipo.int/pressroom/en/articles/2017/article_0002.html.

[164] World Intellectual Property Organization, "U.S. Extends Lead in International Patent and Trademark Filings," press release, March 16, 2016, http://www.wipo.int/pressroom/en/articles/2016/article_0002.html; World Intellectual Property Organization, "Telecoms Firms Lead WIPO International Patent Filings," press release, March 19, 2015, http://www.wipo.int/pressroom/en/articles/2015/article_0004.html; World Intellectual Property Organization, "US and China Drive International Patent Filing Growth in Record-Setting Year," press release, March 13, 2014, http://www.wipo.int/pressroom/en/articles/2014/article_0002.html; World Intellectual Property Organization, "Strong Growth in Demand for Intellectual Property Rights in 2012," press release, March 19, 2013, http://www.wipo.int/pressroom/en/articles/2013/article_0006.html.

[165] China Power Team, "Are Patents Indicative of Chinese Innovation?" China Power, February 15, 2016, updated August 11, 2017, https://chinapower.csis.org/patents/.

[166] China Power Team, "Are Patents Indicative of Chinese Innovation?"

[167] 4G-LTE, or long-term evolution, is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

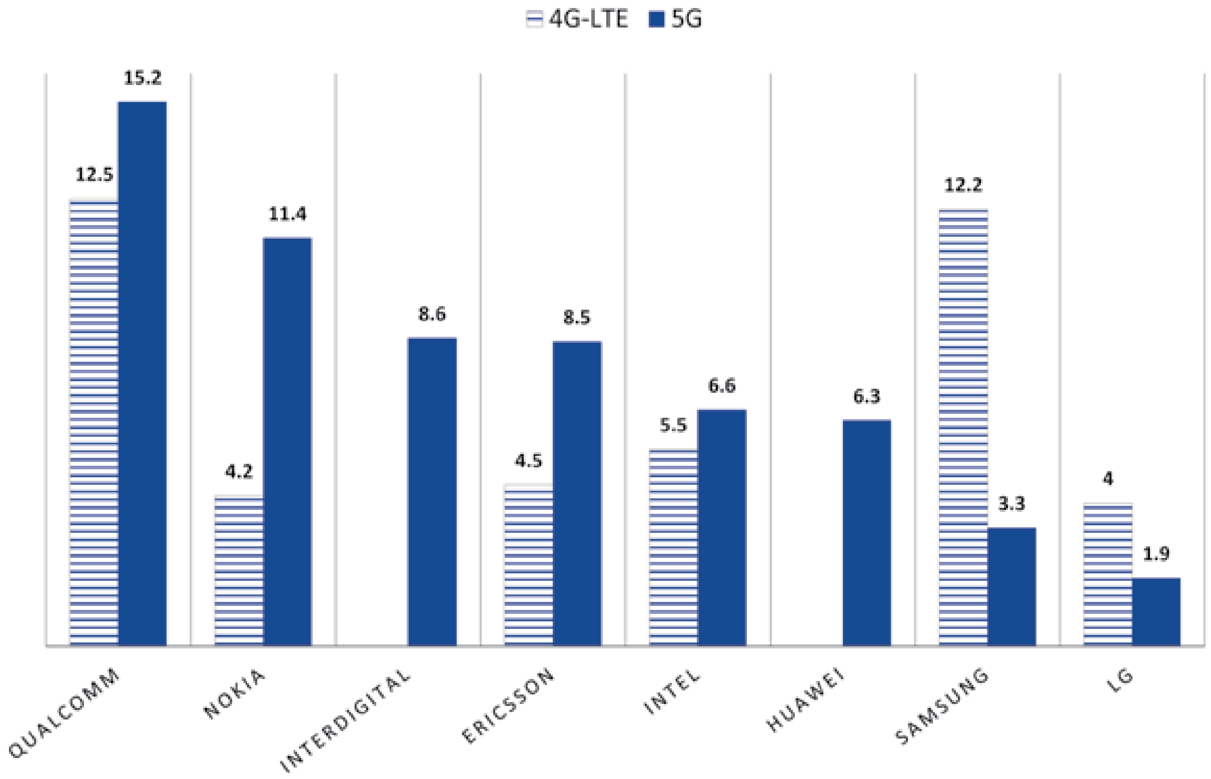
[168] Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017, https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.

[169] Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.

[170] "5G Mobile Network Technology: Patent Landscape Analysis," LexInnova, March 15, 2017, http://www.lex-innova.com/resources-reports/?id=67.

4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 4
Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[171] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the United States.

The creation of 5G standards is divided into two phases. Phase 1 will be finalized by the end of 2017; it is a soft transition phase to 5G that involves backward compatibility with 4G-LTE to protect legacy investments. Phase 2 will be finalized in mid-2018 and will introduce significant changes. Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought

[171] Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV*, http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[172] His four-year term began January 1, 2015, and concludes at the end of 2018. In October 2016, Huawei's Site Energy Efficiency proposal was approved by the ITU.[173] The 3GPP has also accepted Huawei-backed polar code as the coding method for the control channel for 5G Phase 1,[174] and Chinese companies have several proposals in play for Phase 2.[175]

[172] "Biography—Houlin Zhao," International Telecommunication Union, 2017, http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-General of ITU," *China Daily USA*, October 23, 2014, http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

[173] "Huawei's SEE Becomes International Standard after ITU Approval," Huawei, December 5, 2016, http://www.huawei.com/en/news/2016/12/Huawei-SEE-International-Standard-ITU.

[174] Louise Lucas and Nic Fildes, "Huawei Aims to Help Set 5G Standards," *Financial Times*, November 29, 2016, https://www.ft.com/content/f84f968c-b45c-11e6-961e-a1acd97f622d.

[175] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jefferies Hong Kong Limited, September 14, 2017. http://pdf.zacks.com/pdf/JY/H5194437.PDF.

Conclusions

It is unlikely that political or economic shifts will push global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. A national strategy is needed for supply chain risk management of U.S. ICT, and it must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on incident response.

To successfully manage risks associated with Chinese-made products and services and the participation of Chinese companies in ICT supply chains, the U.S. government should:

- ***Establish Centralized Leadership for SCRM***: Threats to U.S. national security posed by state-directed or state-backed adversaries targeting U.S. federal ICT systems will continue, and China's role is in global ICT supply chains is unlikely to change in the near future. In a constrained resource environment, the federal government will need to have a strategy that focuses policy on those threats and vulnerabilities that have the greatest likelihood of occurrence. Establishing a technology-enabled shared SCRM services capability that all federal agencies can access is likely the most cost-effective and impactful means for tackling this evolving threat. A centralized entity for SCRM would need executive-level sponsorship, to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network. This entity's work should be unclassified, but the entity should have a relationship with the intelligence community to ensure collaboration and information sharing.

- ***Embrace an Adaptive SCRM Process***: Federal ICT modernization efforts mean that new products entering the federal information systems and NSS have increasingly complex and globalized supply chains, many of which include commercial suppliers that source from China. These supply chains will change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere.

- ***Promote Supply Chain Transparency***: The government should encourage the public exposure of primary or tier-one suppliers to federal ICT providers and should push for transparency of all suppliers where necessary for certain systems or suppliers at a particular risk or impact level. Suppliers should be required to be transparent about their relationships with entities that are owned, directed, or subsidized by nation states like China, or other entities known to pose a potential supply chain or intelligence threat to the United States. The government should have mechanisms in place and reward industry engagement with these efforts, while establishing consequences for failure to mitigate risk exposure.

- ***Prioritize SCRM throughout the Lifecycle of a Program***: The federal acquisition community should build supply chain transparency requirements or disclosures into ICT procurements from "birth to demise." Having supply chain information on hand earlier and until the end of the program will allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers while the program is operational.

- ***Have a Strategy and Craft Froward-Looking Policy***: Next-generation technologies and standards will have implications for U.S. national security in ways that may not be addressed by existing policies and regulations. Identifying future supply chain risks and addressing them creatively will be important to the success of federal policy efforts. Future risks will likely involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint R&D efforts are also sources of risk not always addressed in traditional SCRM.

Having a strategy that includes these steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from both government and industry. Increased transparency will enhance the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government’s ability to respond to incidents in the event of a supply chain attack, while centralization will reduce the burden facing agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations. Moreover, building supply chain security into policy from the beginning will prevent costly mitigation later, and ensure that federal ICT supply chains—and the federal information systems they supply—remain secure.

Scope Note

This paper is an unclassified report on commercial supply chain vulnerabilities in U.S. federal ICT procurement linked to the People's Republic of China. The study was requested by the U.S.-China Economic and Security Review Commission and is intended as a reference for policymakers, China specialists, and supply chain professionals on how the U.S. government manages risks associated with Chinese-made products and services and the participation of Chinese companies in U.S. ICT supply chains. The research for this project covered three major connection routes between China and U.S. federal ICT supply chains and the risks those connections pose to U.S. national security. Sources used in this paper may refer to information technology, which can include computers, software, electronics, and other information distribution technologies. This paper's scope addresses the more expansive category of ICT, which encompasses audio-visual communications systems, data storage, and other integration technologies.

METHODOLOGY

This study defines "U.S. government ICT supply chains" as (1) primary suppliers, (2) tiers of suppliers that support primary suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. This comprehensive definition includes supply chains that are multi-tiered, webbed relationships in addition to those that are singular or linear in nature. The greatest risk is often found in the second or third tiers of a supply chain and in indirect relationships within the chain.

The Commission requested a study that reviewed laws, regulations, and other requirements since the passage of FITARA in February 2014. The study includes detailed recommendations to minimize the risk that the Chinese government, Chinese companies, or Chinese products may pose to U.S. federal ICT supply chains. Interos supply chain risk analysts and China experts were specifically tasked by the Commission to assess—

1. China's role in the global ICT supply chain and China's participation in U.S. federal ICT supply chains, including U.S. government reliance on Chinese firms, products, and services and the risk those products and services pose to U.S. economic health and national security

2. Cases in which the Chinese government, Chinese companies, or Chinese products have been implicated in connection with U.S. supply chain vulnerabilities or exploitation

3. Current U.S. government efforts to manage risk from foreign-made products and foreign firms participating in its IT procurement, including differences between non-national-security-related and national-security-related ICT procurement

4. Points of vulnerability and loopholes in the existing U.S. federal risk management system, including prospects for future development as Chinese manufacturing, research, and development capabilities evolve

Included in this report are seven of the largest providers of enterprise IT to the U.S. federal government that are also ICT OEMs: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[176] This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although all of these companies conduct some level of due diligence on their supplier base, their complete records are not publicly available.

[176] "Top 25 Enterprise IT Providers," FedScoop.

SOURCES

The source material for this study is unclassified, publicly available, open source information, to include information from media, the internet, public government data, academic and industry publications, and commercial databases. For some subjects, the implications of unclassified information are highly suggestive yet inconclusive. For example, unclassified information is often insufficient to conclusively attribute ICT network intrusions and telecommunications supply chain vulnerabilities to the Chinese government, Chinese companies, or Chinese products. The analysis and attributions in this study present the best available unclassified information, with appropriate caveats when necessary.

The Chinese source material for the study came from authoritative PRC publications and authors, including government-affiliated press entities, and from the Chinese- and English-language web pages of Chinese companies, including defense providers and ICT suppliers.

Additional data used in the supply chain analysis of major U.S. federal ICT suppliers were obtained from relevant open source intelligence, including social media, free and subscription services, and other structured and unstructured data sources.

The result is a comprehensive review of the links between major U.S. federal ICT suppliers and the Chinese government, Chinese companies, and Chinese products that may pose a risk to U.S. federal ICT supply chains.

Acknowledgments

Interos Solutions would like to thank the U.S.-China Economic and Security Review Commission for its support of this research and the opportunity to present these findings. That said, we could not have produced this report without help from others. Our thanks are also due to Tara Madison, Sheila Gagen, Johanna Daproza, and other members of Vector Talent Resources for their editorial and design support.