U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

July 27, 2017

Congressional Committees

State Department Telecommunications: Information on Vendors and Cyber-Threat Nations

Reliance on complex, global information technology (IT) supply chains introduces multiple risks to federal telecommunications systems, including the risk of these systems being manipulated or damaged by leading foreign cyber-threat nations (cyber-threat nations) such as China, Iran, North Korea, and Russia.[1] Threats and vulnerabilities created by these cyber-threat nations and other malicious actors can be sophisticated and difficult to detect, and thus pose a significant risk to organizations and federal agencies. Such supply chain risks may include the insertion of counterfeits, tampering, or installation of malicious software or hardware.

The federal government views dependence on foreign-manufactured equipment as an emerging threat that introduces potential risks to agency networks. Although it is impossible to completely eliminate all risks, the federal government has taken some steps to mitigate supply chain risks. Agencies are required by the Federal Acquisition Regulation (FAR) to ensure that contracts include quality requirements that are determined necessary to protect the government's interest. The National Institute of Standards and Technology (NIST) has prescribed guidance intended to mitigate supply chain risks.[2] The Department of State (State) has also enacted agency policies that broadly reflect federal law and guidance; these policies are intended to operationalize the federal rules and regulations.[3] We have previously reported on risks to the IT supply chain, as well as risks originating from foreign-manufactured equipment.[4]

[1]In this report, *telecommunications* encompasses the "preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means," as defined by the Committee on National Security Systems Glossary, Instruction No. 4009 (Ft. Meade, Md.: Apr. 6, 2015). The Office of the Director of National Intelligence identifies China, Iran, North Korea, and Russia as leading cyber-threat nations in its *Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 9, 2016).

[2]NIST developed Special Publication (SP) 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Gaithersburg, Md.: Department of Commerce, 2015). Its intent is to assist federal agencies with identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations. Additionally, the FAR, established for the codification and publication of uniform policies and procedures for acquisition by all executive branch agencies, provides government-wide regulation and is implemented by relevant agency policies and procedures.

[3]State's Acquisition Regulation implements and supplements the FAR, while its *Foreign Affairs Manual* and supplementary *Foreign Affairs Handbooks* include provisions for supply chain risk management.

[4]GAO, *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment*, GAO-13-652T (Washington, D.C.: May 21, 2013) and *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

The Department of State Authorities Act, Fiscal Year 2017 (State Authorities Act), includes a provision for us to review State's critical telecommunications equipment or services obtained from vendors,[5] or those vendors' contractors or subcontractors, that are closely linked to leading cyber-threat nations.[6] The Office of the Director of National Intelligence identified China, Iran, North Korea, and Russia as leading cyber-threat nations. The State Authorities Act defines "closely linked" as, with respect to a foreign supplier, contractor, or subcontractor and a cyber-threat nation,

> (A) incorporated or headquartered in the territory;
>
> (B) having ties to the military forces;
>
> (C) having ties to the intelligence services; or
>
> (D) the beneficiary of significant low-interest or no-interest loans, loan forgiveness, or other support of a leading cyber-threat nation.

This report identifies telecommunications equipment or services acquired or used by State that may have been obtained from entities reported to be closely linked to cyber-threat nations as defined in the State Authorities Act. Our examination includes a review of companies that manufacture equipment or develop software applications supporting State's critical telecommunications capabilities (device manufacturers or software developers), as well as companies contracted to support State's telecommunications capabilities (telecommunications contractors), irrespective of criticality.

We examined generalizable samples of State's critical telecommunications device manufacturers and software developers, as well as State's telecommunications contractors, to identify potential links between these vendors and cyber-threat nations, as reported in open sources.

- To identify the companies that manufacture critical telecommunications equipment acquired or used by State, we asked State to create a list of current device manufacturers and software developers that currently support the agency's telecommunications capabilities. State reported that it determines system criticality against criteria established for *mission critical* systems released by NIST Special Publication 800-60,[7] or for *critical infrastructure*, as defined by Committee on National Security Systems (CNSS) Instruction 4009.[8] We reviewed this list and drew a

[5]In this report, the term *vendor* includes State's critical telecommunications equipment manufacturers and software developers, as well as State's telecommunications contractors.

[6]Pub. L. No. 114-323, § 707.

[7]In this report, we define *mission critical* as follows: "Any telecommunications or information system that is defined as a national security system (Federal Information Security Modernization Act (FISMA)) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency." See *Guide for Mapping Types of Information and Information Systems to Security Categories,* NIST Special Publication 800-60 (Gaithersburg, Md.: August 2008).

[8]In this report, we define *critical infrastructure* as follows: "System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." See Committee on National Security Systems Glossary, Instruction No. 4009 (Ft. Meade, Md.: April 6, 2015).

generalizable sample of 52 randomly selected unique device manufacturers and software developers out of the 111 identified by State as supporting its critical telecommunications capabilities.

- To identify State's telecommunications contractors, we queried all State telecommunications-related contracts in the Federal Procurement Data System-Next Generation (FPDS-NG) awarded from January 2014 through March 2017. We selected this time frame to account for current and multi-year contracts. The awarded contracts could not be segmented by the criticality of the equipment or services procured because these data were not available in FPDS-NG. We reviewed the list of 959 contractors and drew a generalizable sample of 100 randomly selected unique awardees of State's telecommunications contracts within our time frame.

- To determine whether the State-identified device manufacturers and software developers and State telecommunications contractors had potential close links, as defined by the State Authorities Act, to cyber-threat nations, we conducted an open source review of publicly available information for each of our sampled vendors. Specifically, we used the Bloomberg Terminal's supply chain analysis function to query which of State's telecommunications vendors—or their suppliers—were reported to be headquartered in leading cyber-threat nations. We used Lexis-Nexis to query which of State's telecommunications vendors—or their suppliers—were reported to have any military ties, intelligence ties, or low-interest loans with leading cyber-threat nations.

While we were able to identify State's telecommunications device manufacturers, software developers, and contractors, the data available to us in the open source searches of our two samples did not establish whether these vendors' suppliers provided equipment or services directly supporting the agency's critical telecommunications capabilities. See the enclosure for a full description of our scope and methodology.

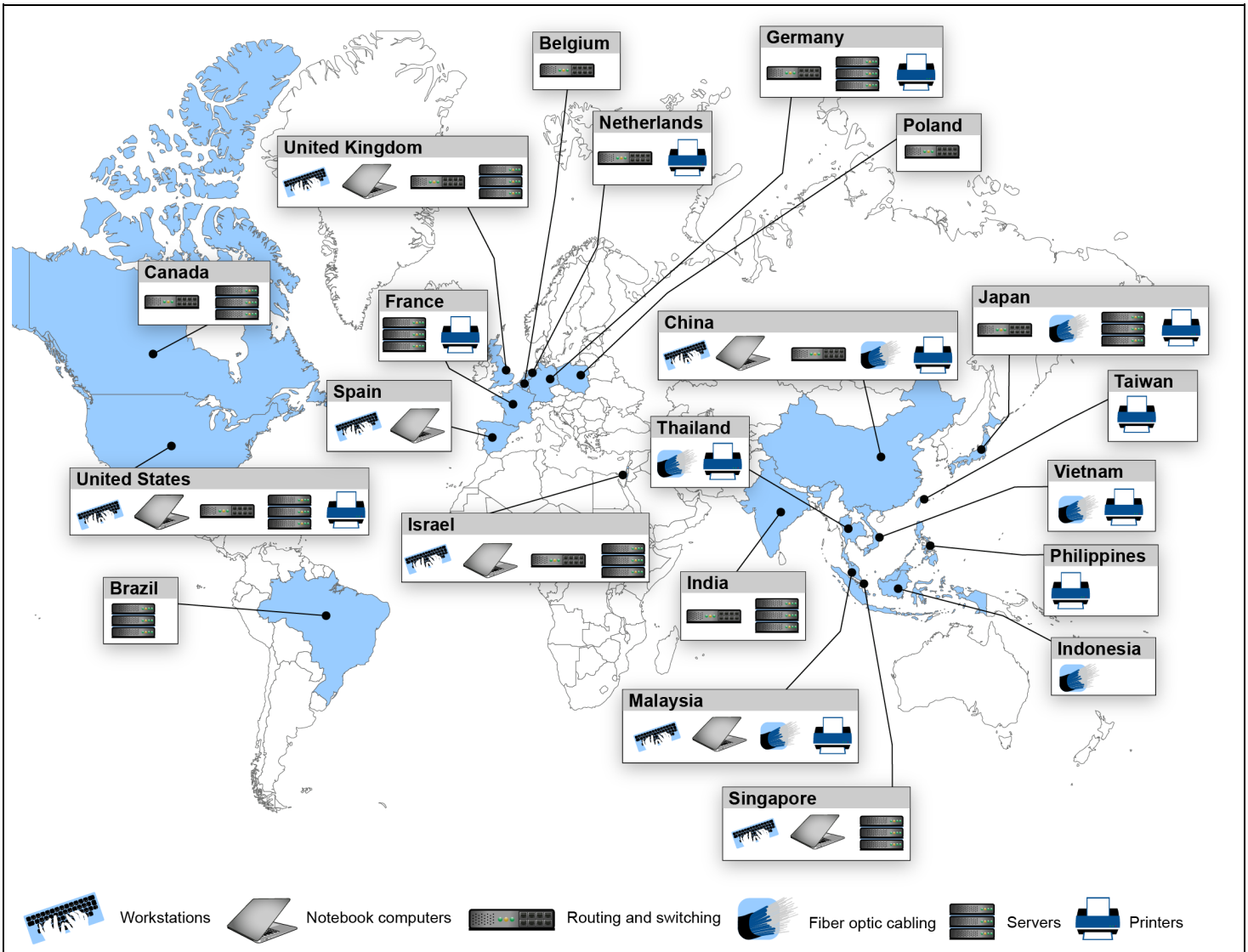
We conducted this performance audit from February 2017 to July 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The federal government relies heavily on IT equipment manufactured in foreign nations. Federal telecommunications systems can include a multitude of IT equipment, products, and services, each of which may rely on one or more supply chains. These supply chains can be long, complex, and globally distributed and can consist of multiple tiers of outsourcing.

Typical telecommunications networks include a variety of commercial-off-the-shelf products that have been sourced from across the world. Many of these products, or their subcomponents, originate in Asia, with China as the largest importer and exporter of IT hardware globally. As a result, agencies may have little visibility into, understanding of, or control over how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to ensure the integrity, security, resilience, and quality of the products and services. Figure 1 highlights possible manufacturing locations of typical network components.

Figure 1: Possible Manufacturing Locations of Typical Network Components



Source: GAO analysis of public information. | GAO-17-688R

Component	Possible manufacturing locations
Workstations	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Notebook computers	United States, Israel, Spain, China, Malaysia, Singapore, United Kingdom
Routing and switching	United States, India, Belgium, Canada, China, Germany, Israel, Japan, Netherlands, Poland, United Kingdom
Fiber optic cabling	China, Malaysia, Vietnam, Japan, Thailand, Indonesia
Servers	Brazil, Canada, United States, India, Japan, France, Germany, United Kingdom, Israel, Singapore
Printers	Japan, United States, Germany, France, Netherlands, Taiwan, China, Malaysia, Thailand, Vietnam, Philippines

State's Critical Telecommunications Device Manufacturers and Software Developers, and State's Telecommunications Contractors

State's Critical Telecommunications Device Manufacturers and Software Developers

Based on our open source review of a generalizable sample of 52 unique State telecommunications device manufacturers and software developers, we did not identify any reported close links to cyber-threat nations as defined by the State Authorities Act.[9]

Of the 52 manufacturers or software developers in our sample, we were able to identify 12 that had 1 or more suppliers that were reported to be headquartered in a leading cyber-threat nation. We identified a total of 74 such suppliers; all but one of these suppliers reported having their headquarters in China. For example, for one manufacturer of telecommunications devices, our open source review reported 48 such suppliers: 47 were reported to be headquartered in China, and 1 was reported to be headquartered in Russia. Accordingly, we estimate that 23 percent of all State telecommunications device manufacturers and software developers have at least 1 supplier reported to be headquartered in a leading cyber-threat nation.[10]

Our open source review could not indicate whether these suppliers provided equipment or services directly supporting State's critical telecommunications capabilities. There were 25 publicly traded companies and 27 privately held companies in our sample. While we searched for reported supply chain information in the Bloomberg data for both types of company, we did not find any for the privately held companies.[11]

Based on our open source review, we did not identify any reported military ties, intelligence ties, or low-interest loans involving cyber-threat nations among any of the suppliers to our sample of device manufacturers and software developers.[12]

State's Telecommunications Contractors

Based on our open source review of a generalizable sample of 100 State telecommunications contract awardees, we did not identify any reported close links to cyber-threat nations as defined by the State Authorities Act.[13]

Of the 100 contractors in our sample, we were able to identify 4 that had 1 or more suppliers reported to be headquartered in a cyber-threat nation. We identified a total of 28 such suppliers,

[9]We estimate with 95 percent confidence that 0 percent to 5 percent of our total population of 111 may be directly linked to cyber-threat nations.

[10]The margin of error on the estimate of 23 percent is plus or minus 9 percentage points.

[11]A representative from Bloomberg's Supply Chain Data team told us that it is more difficult for them to obtain supply chain information for the privately held companies, as privately held companies are generally not governed by disclosure mandates as are publicly held companies.

[12]The Lexis-Nexis search we conducted did not allow us to search specifically for supply chain relationships but our query regarding whether State's telecommunications vendors—or their suppliers—were reported to have any military ties, intelligence ties, or low-interest loans with leading cyber-threat nations potentially could have identified some supply chain relationships.

[13]We estimate with 95 percent confidence that 0 percent to 3 percent of our total population of 959 may be directly linked to cyber-threat nations.

and all of them were reported as having their headquarters in China. One contractor of telecommunications devices had 18 such suppliers, while the remaining three contractors were reported to have 5, 4, and 1 Chinese suppliers, respectively. Accordingly, we estimate that 4 percent of all State telecommunications contractors had 1 or more suppliers reported to be headquartered in a leading cyber-threat nation.[14]

Our open source review could not determine whether these suppliers provided equipment or services directly supporting State's critical telecommunications capabilities.[15] There were 6 publicly traded companies and 94 privately held or other companies in our sample. While we searched for reported supply chain information in the Bloomberg data for both types of company, we did not find any for the privately held companies.[16]

Based on our open source review we did not identify any reported military ties, intelligence ties, or low-interest loans involving cyber-threat nations among any of the suppliers to our sample of contractors.[17]

Agency Comments

We provided a draft of this report to the Department of State for comment. State provided a technical comment, which we incorporated as appropriate.

- - - - -

[14]The margin of error on the estimate of 4 percent is no greater than 6 percentage points.

[15]We did not identify any reported military ties, intelligence ties, or low-interest loans involving cyber-threat nations among any of the suppliers to our sampled contractors.

[16]A representative from Bloomberg's Supply Chain Data team told us that it is more difficult for them to obtain supply chain information for the privately held companies, as privately held companies are generally not governed by disclosure mandates as are publicly held companies.

[17]The Lexis-Nexis search we conducted did not allow us to search specifically for supply chain relationships, but our query regarding whether State's telecommunications vendors—or their suppliers—were reported to have any military ties, intelligence ties, or low-interest loans with leading cyber-threat nations potentially could have identified some supply chain relationships.

We are sending copies of this report to the Secretary of State, appropriate congressional committees, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you and your staff have any questions, please contact Michael J. Courts at (202) 512-8980 or courtsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributors to this report were Thomas Costa (Assistant Director), Wayne Emilien (Analyst-in-Charge), Amanda Bartine, JoAnna Berry, Debbie Chung, Martin de Alteriis, Mark Dowling, Justin Fisher, Nicholas Jepson, Julia Kennon, Mary Moutsos, Dwayne Staten, and Elaine Vaurio.

Michael J. Courts
Director, International Affairs and Trade

Enclosure

List of Committees

The Honorable Bob Corker
Chairman
The Honorable Benjamin L. Cardin
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Ed Royce
Chairman
The Honorable Eliot L. Engel
Ranking Member
Committee on Foreign Affairs
House of Representatives

Enclosure

Objective, Scope, and Methodology

The Department of State Authorities Act, Fiscal Year 2017 (State Authorities Act), includes a provision for us to report on State's critical telecommunications equipment or services obtained from vendors,[18] or those vendors' contractors or subcontractors, that are closely linked to leading cyber-threat nations.[19] The *Worldwide Threat Assessment of the U.S. Intelligence Community* published in February 2016 by the Office of the Director of National Intelligence identifies China, Iran, North Korea, and Russia as such nations. [20]

Our objective was to identify critical telecommunications equipment or services acquired or used by the Department of State (State) that may have been obtained from entities closely linked to a leading foreign cyber-threat nation (cyber-threat nation).

The State Authorities Act defined "closely linked" as, with respect to a foreign supplier, contractor, or subcontractor and a cyber-threat nation,

- incorporated or headquartered in the territory;
- having ties to the military forces;
- having ties to the intelligence services; or
- the beneficiary of significant low-interest or no-interest loans, loan forgiveness, or other support of such nation.

We defined telecommunications as the "preparation, transmission, communication, or related processing of information (writing, images, sounds, or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means."[21]

We defined a critical system as meeting one of two thresholds:

- Mission critical: "Any telecommunications or information system that is defined as a national security system by the Federal Information Security Modernization Act, or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency,"[22] or
- Critical infrastructure: "System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a

[18]In this report, the term *vendor* includes State's critical telecommunications equipment manufacturers and software developers, as well as State's telecommunications contractors.

[19]Pub. L. No. 114-323, § 707.

[20]*Worldwide Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Feb. 9, 2016).

[21]Committee on National Security Systems Glossary, Instruction No. 4009 (Ft. Meade, Md.: Apr. 6, 2015).

[22]*Guide for Mapping Types of Information and Information Systems to Security Categories*, NIST Special Publication 800-60 (Gaithersburg, Md.: August 2008).

> debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[23]

To address our objective, we first sought to identify the critical equipment, software, or services acquired or in use by State. We examined generalizable samples of (1) critical telecommunications equipment manufacturers and software developers from a list that State provided, and (2) all State telecommunications contracts found in the Federal Data Procurement System-Next Generation (FPDS-NG) database of government contracts. These two samples, helped ensure that we examined (1) manufacturers and software developers of its existing telecommunications inventory that State deemed critical and (2) all of State's telecommunications equipment contractors from January 2014 through March 2017. We only used publicly available sources and data to identify possible links between these vendors and cyber-threat nations.

In this report, we defined supply chain relationships as a quantifiable financial link between device manufacturers, software developers, and contractors with any of their suppliers, as reported in Bloomberg from public sources, such as U.S. Security and Exchange Commission filings and annual or semiannual reports.

We requested a copy of State's current inventory of general support systems and applications supporting its critical telecommunications capabilities. We also requested a list of State's equipment and services supporting these systems including manufacturer or service provider and country of origin. State provided us with a list of two systems—along with their related devices and software—that they determined to be critical. This list included 111 unique telecommunications device manufacturers and software developers from which we derived our sample.

To assess the reliability of State's list of device manufacturers and software developers, we questioned and received written responses from State officials about their databases that contain this information, and reviewed the list for duplicate entries, errors, and incomplete entries. We found 18 invalid entries in the data and excluded those from our sample. We determined that the resulting data provided a reliable list of manufacturers and software developers that State reported as supporting its critical telecommunications capabilities.

We drew a random sample consisting of 52 of the device manufacturers from this list that was designed to be generalizable to the population of the list that State provided. Of these, 25 were publicly traded companies, and 27 were privately held companies.

We estimate with 95 percent confidence that 0 percent to 5 percent of our total population of 111 may be directly linked to leading cyber-threat nations. We also estimate with 95 percent confidence that 23 percent of the population of 111 may have one or more suppliers that are headquartered in a cyber-threat nation, with confidence intervals of plus or minus 9 percent.

In addition to reviewing the device manufacturers and software developers, we used FPDS-NG to select a generalizable sample of 100 telecommunications contracts awarded by State from January 2014 through March 2017. We selected this time frame in order to account for current contracts, multiyear contracts, and contracts that may have recently ended.

[23]Committee on National Security Systems Glossary, Instruction No. 4009.

We included this sample in our review to determine any possible linkage between State's contract vendors or subcontractors to cyber-threat nations because the list of device manufacturers that State provided did not include its corresponding telecommunications contract information. Further, because we compiled this sample from FPDS-NG, which does not identify the criticality of contracts, we were unable to determine the criticality of the telecommunications systems that the contract vendors support.

To draw our generalizable sample of State contract vendors, we queried all State telecommunications-related contracts listed in FPDS-NG awarded within our time frame, a total of 5,226. We chose FPDS-NG because it has served as the primary federal procurement database since 1978.[24] We then filtered the dataset to only include contracts where both industry codes—the North American Industry Classification System (NAICS) and Product Service Codes (PSC)—were related to telecommunications, and only unique vendors.[25]

To assess the reliability of the FPDS-NG data, we reviewed available documentation on how the data are gathered and checked and performed basic logic checks. We determined the FPDS-NG data were sufficiently reliable for the purpose of identifying State's telecommunications contracts and the vendors that State had contracted with.

With our resulting population of 959 vendors, we drew a random sample of 100 sample vendors, whose results were generalizable across the entire population. Of these, 6 were public companies and 94 were privately held or other companies.

---

[24]Congress, executive branch agencies, and the public can use FPDS-NG for a broad range of data on agency contracting actions, procurement, and spending. FPDS-NG can be accessed at https://www.fpds.gov/fpdsng_cms/. Reporting requirements for FPDS-NG are in Federal Acquisition Regulation (FAR) subpart 4.6; FPDS-NG data are described in FAR 4.602. The Office of Management and Budget established FPDS-NG, and the U.S. General Services Administration administers the system. For more information on FPDS-NG and other federal procurement data systems, see GAO, *Federal Contracting: Observations on the Government's Contracting Data Systems*, GAO-09-1032T (Washington, D.C.: Sept. 29, 2009).

[25]We included the following NAICS codes in our sample:

- telephone apparatus manufacturing; software and other prerecorded compact disc, tape, and record reproducing; semiconductor and related device manufacturing; search, detection, navigation, guidance, aeronautical, and nautical system and instrument manufacturing; radio and television broadcasting and wireless communications equipment manufacturing; printed circuit assembly (electronic assembly) manufacturing; other measuring and controlling device manufacturing; other electronic component manufacturing; other computer related services; other communications equipment manufacturing; irradiation apparatus manufacturing; instruments and related products manufacturing for measuring, displaying, and controlling industrial process variables; instrument manufacturing for measuring and testing electricity and electrical signals; electronic connector manufacturing; electronic computer manufacturing; electro-medical and electrotherapeutic apparatus manufacturing; custom computer programming services; computer terminal and other computer peripheral equipment manufacturing; computer systems design services; computer storage device manufacturing; computer facilities management services; computer and software stores; computer and office machine repair and maintenance; computer and computer peripheral equipment and software merchant wholesalers; capacitor, resistor, coil, transformer, and other inductor manufacturing; blank magnetic and optical recording media manufacturing; automatic environmental control manufacturing for residential, commercial, and appliance use; audio and video equipment manufacturing; analytical laboratory instrument manufacturing; and all other telecommunications.

We also included the following PSCs in our sample:

- communication, detection, and coherent radiation equipment; electrical and electronic equipment components; fiber optics materials, components, assemblies and accessories; electric wire and power and distribution equipment; and information technology services, including telecommunications services.

We estimate with 95 percent confidence that 0 percent to 3 percent of our total population of 959 may be directly linked to cyber-threat nations. We also estimate with 95 percent confidence that 4 percent of our total population of 959 may have one or more suppliers reported to be headquartered in a cyber-threat nation, with a confidence interval of between 2 percent to 10 percent.

To determine whether any of the vendors in either of our samples were reported to have possible links, as defined by the State Authorities Act, to cyber-threat nations, we utilized Bloomberg's supply chain analysis function to conduct an open source—that is, overt and publicly available—review of our generalizable samples. We assessed whether each of our vendors, or their suppliers, were reported to be incorporated or headquartered in cyber-threat nations. Doing so allowed us to identify the country of incorporation or headquarters for the manufacturers and developers, as well as their suppliers, as reported in Bloomberg. The publicly available information included the relationships of the vendors in our sample to their suppliers, which allowed us to search for instances where State's manufacturers and/or their suppliers were reported to be headquartered in the countries identified as cyber-threat nations. A representative from Bloomberg told us that manufacturing can often take place in countries other than the one in which a supplier is headquartered; however, the data did not allow us to search based on manufacturing locale. The Bloomberg data also did not allow us to search systematically to determine if the sampled manufacturers were reported to have ties to the military forces, intelligence services, or were the beneficiary of loan assistance from cyber-threat nations.

To determine the reliability of Bloomberg's supply chain analysis function in identifying supply chain relationships and each company's and supplier's country of domicile, we reviewed documentation provided by Bloomberg and interviewed a representative from Bloomberg's Supply Chain Data team. When identifying reported supply chain relationships, we used the standard established by Bloomberg for quantifiable relationships—those relationships where Bloomberg could quantify the percentage of revenue earned as a result of transactions between our sampled companies and their suppliers. We determined these data to be sufficiently reliable to determine publicly reported supply chain relationships and to identify companies that are reported to be incorporated or headquartered in cyber-threat nations. The publicly available information allowed us to search for instances where State's vendors and their suppliers were reported to be headquartered in the nations identified as cyber-threat nations. We searched the Bloomberg data for both publicly traded and privately held companies for supply chain information. However, a representative from Bloomberg told us that it is more difficult for them to obtain that information for privately held companies, and we did not find any information on the privately held companies' supply chain relationships. For the vendors' suppliers, we could establish whether they were reported to be headquartered in cyber-threat nations but could not determine whether State's device manufacturers, software developers, and contractors had purchased any products or services from those suppliers.

Because the Bloomberg supply chain analysis function only provided supply chain information for publicly traded companies and did not allow us to search for reports of vendors having ties to the military forces or intelligence services, or reports of vendors who were the beneficiaries of significant low-interest or no-interest loans, loan forgiveness, or other support of such nations, we continued the searches for the names of both publicly and privately held vendors included in our sample using Lexis-Nexis (broad U.S. News and World Report publication files to cover the largest amount of open source information). We searched company names that appeared within 15 (w/15) words from "China," "Russia," "Iran," or "North Korea" and within 15 (w/15) words from "intelligence," "military," or "loans." In instances where our Lexis-Nexis search identified possible

reported close links, as defined by the State Authorities Act, between the manufacturers and cyber-threat nations, we planned to require two sources corroborating the information if one of the sources was published by the manufacturer. If none of the sources were published by the manufacturer, we planned to require three sources to corroborate potential reported linkage between the manufacturer and a cyber-threat nation. However, our Lexis-Nexis searches did not identify any corporations that met our criteria.

The open source searches did not establish whether State directly purchased equipment or services from any of the suppliers linked to our two samples of vendors.

We conducted this performance audit from February 2017 to July 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(101661)