Statement of

Robert C. Erickson, Jr.

Deputy Inspector General

U.S. General Services Administration

before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

concerning

Made in China: Is GSA Complying with Purchasing Restrictions?

February 29, 2024

Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee:

Thank you for the opportunity to testify today regarding recent technology-related reports issued by the Office of Inspector General (OIG) to the management of the General Services Administration (GSA).

The Inspector General Act of 1978 establishes, within most major federal agencies, an office of Inspector General to promote economy and efficiency; prevent and detect waste, fraud, and mismanagement; and to exercise important law enforcement functions related to the programs and operations of those agencies. It is under this authority that the OIG audits GSA's information technology.

As requested by the Subcommittee, my testimony today will briefly summarize three of our recent audit reports:

- *GSA Purchased Chinese-Manufactured Videoconference Cameras and Justified It Using Misleading Market Research*, issued in January 2024;
- *Multiple Award Schedule Contracts Offered Prohibited Items, Putting Customers at Risk of Unauthorized Surveillance by Foreign Adversaries*, issued in July 2023; and
- *Audit of Security Controls for Mobile Technologies Used by GSA*, issued in September 2023.

The first two reports are available on our website and Oversight.gov. We issued the third report to GSA management as a restricted report. This report is not publicly available because it contains sensitive information that, if disclosed, might adversely affect information technology security.

Purchase of Chinese Cameras Justified with Misleading Research

In recent years, our office has seen an increase in alleged violations of the Trade Agreements Act (TAA) of 1979, 19 U.S.C. Chapter 13. These generally involve contractors falsely claiming their products are TAA-compliant. In this case, however, GSA purchased products they knew were made in China as part of a pilot project. This pilot project was designed to determine whether the products should be purchased for use throughout GSA.

Background: TAA and the Federal Acquisition Regulation

The TAA was enacted on July 26, 1979, to foster fair and open international trade. This act requires the federal government to purchase only goods that are manufactured in the United States or a TAA-designated country, with limited exceptions. China is not a TAA-designated country.

In implementing this law, the Federal Acquisition Regulation (FAR) requires that the government consider only "U.S.-made or designated country end products unless the contracting officer determines that there are no offers for such products or that the offers for those products are insufficient" to meet the government's needs.

Initiation of the OIG Audit

In 2022, our office was contacted by a GSA employee who was concerned about GSA's purchase and use of Chinese-manufactured videoconference cameras. The employee asserted that because these cameras were manufactured in China, they were not compliant with the TAA. We initiated an audit to determine whether GSA's purchase and use of these Chinese-manufactured videoconference cameras were in accordance with federal laws, regulations, and internal guidance.

Findings and Recommendations

Our auditors found that GSA Office of Digital Infrastructure Technologies (IDT) employees misled a contracting officer, the GSA employee responsible for the purchase, with egregiously flawed information to acquire 150 Chinese-manufactured, TAA-noncompliant videoconference cameras. GSA purchased 70 of the TAA-noncompliant cameras in March 2022, followed by an additional purchase of 80 TAA-noncompliant cameras in October 2022.

Before completing the purchases, the contracting officer requested information from GSA IDT to justify its request for the TAA-noncompliant cameras, including the existence of TAA-compliant alternatives and the reason for needing the specified brand. In response, GSA IDT provided misleading market research in support of the TAA-noncompliant cameras and failed to disclose that comparable TAA-compliant alternatives were available.

The TAA-noncompliant cameras have known security vulnerabilities that need to be addressed with a software update. As of our report issuance, GSA records indicated that some of these TAA-noncompliant cameras had not been updated and remained susceptible to these security vulnerabilities.

As of September 18, 2023, there were 210 active TAA-noncompliant cameras registered to GSA email addresses. Of the 210 cameras, 29 (14 percent) had not been updated to address known security vulnerabilities.

Other notable findings include the following:

- The second purchase of TAA-noncompliant cameras, which included 80 additional cameras, occurred in October 2022 despite GSA personnel's knowledge that we were reviewing their March 2022 purchase.

- The GSA contracting officer who approved the purchase of the cameras stated that if she had been provided with accurate market research, including information about the existence of TAA-compliant products that met the requirements, then the FAR would have required her to consider only the TAA-compliant cameras for purchase.

- The TAA-noncompliant cameras were also offered on the GSA Multiple Award Schedule (MAS), incorrectly listing the country of origin as Taiwan. During the audit, we notified the MAS contracting officer that the country of origin was actually China.

The MAS contracting officer requested that the contractor remove the cameras on October 11, 2022.

In our audit report, we made four recommendations to GSA leadership:

First, we recommended that GSA ensure that the agency no longer purchase TAA-noncompliant cameras if there are TAA-compliant cameras that meet the government's requirements.

Second, we recommended that GSA return, or otherwise dispose of, previously purchased TAA-noncompliant cameras.

Third, we recommended that GSA strengthen controls to ensure that TAA-compliant products are prioritized during future procurements, contracting officer determinations are adequately reviewed prior to approval, appropriate determinations are obtained before the purchase of noncompliant products, and IT equipment is updated in a timely manner to reduce the risk of overlooking identified vulnerabilities.

Finally, we recommended that GSA take appropriate action against the responsible agency personnel to address the misleading information provided to the contracting officer for the purchase of TAA-noncompliant cameras.

Agency leadership, including the Chief Information Officer (CIO), agreed with our recommendations, except for the recommendation that the agency return, or otherwise dispose of, the TAA-noncompliant cameras.

In their written comments in response to our draft report, agency leadership wrote that they are confident that GSA's current security protocols are sufficient to secure the TAA-noncompliant cameras. They stated that those security protocols included discontinuing the use of some TAA-noncompliant cameras that do not meet GSA's standards.

We considered the agency's comments carefully prior to issuance of the final report but, due to security and procurement concerns, decided to reaffirm our recommendation that GSA should return or dispose of these TAA-noncompliant cameras. The agency's written comments are included in their entirety as an appendix to the audit report, which is available on both our website and Oversight.gov.

Audit Follow-Up

As required by internal GSA policy, GSA leadership must provide us a corrective action plan for implementing our report recommendations. GSA's corrective action plan for this report is due to our office on March 25. We will review GSA's plan and notify them whether we find their proposed actions are responsive to the recommendations we have made.

Prohibited Items on the Multiple Award Schedule

In July 2023, we issued the audit report titled, *Multiple Award Schedule Contracts Offered Prohibited Items, Putting Customers at Risk of Unauthorized Surveillance by Foreign Adversaries.*

Background

GSA's Federal Acquisition Service (FAS) is responsible for ensuring regulatory compliance for items that contractors offer on its MAS contracts. This is especially important with the increase in national security and intellectual property threats to the federal government's supply chain.

The National Defense Authorization Acts for 2018 and 2019 prohibit the federal government's procurement, or use of certain telecommunications (telecom) and video surveillance services or equipment from six different companies, their subsidiaries, or affiliates. In accordance with these laws, the FAR restricts MAS contractors from providing or using any prohibited telecom items from those same entities. These prohibited telecom items could be used by foreign adversaries for unauthorized surveillance. We performed this audit to determine whether FAS is complying with laws, regulations, and policies to ensure that MAS contracts do not offer prohibited telecom items.

Between October 2018 and February 2022, the federal government spent approximately $7 billion on telecom items procured through GSA's MAS program.

Findings and Recommendations

Our audit found prohibited telecom items on MAS contracts. Two of the primary methods that FAS relies on to ensure that MAS contracts do not include these items are contractor self-certifications and an automated process that flags potentially prohibited telecom items included on GSA's online shopping service, GSA Advantage! However, the self-certifications are inadequate, and the automated flagging process is insufficient to prevent contractors from including prohibited telecom items on their MAS contracts. The audit team also found problems with FAS's efforts to address prohibited telecom items offered on MAS contracts, including:

- FAS has not taken adequate actions against contractors that repeatedly violate the FAR restrictions on providing or using prohibited telecom items;

- FAS does not have a process in place to notify customer agencies about their purchases of prohibited telecom items; and

- FAS did not initially comply with FAR requirements to include subsidiaries and affiliates of named entities in its efforts to identify prohibited telecom items on MAS contracts.

We made five recommendations for corrective action. In its seven-page response to our report, GSA fully concurred with all of our recommendations and provided general comments on its

internal controls and efforts related to prohibited telecom items. We included GSA's response as an appendix to our report, which is available on our website and Oversight.gov.

We received and accepted GSA's corrective action plan for implementing the recommendations. GSA is responsible for completing the corrective actions.

Security Controls for GSA Mobile Devices

As part of our Fiscal Year 2022 Audit Plan, we performed an audit to determine whether GSA's Office of the Chief Information Officer (GSA IT) has addressed cybersecurity risks to its mobile technologies in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and the agency's own internal security policy.

Upon completion of the audit, we issued an audit report to GSA management in September 2023. The report, *Audit of Security Controls for Mobile Technologies Used by GSA,* is not available to the public because it contains sensitive information that, if disclosed, might adversely affect information security.

Like many large organizations, GSA IT manages thousands of mobile devices, including smartphones and tablets, used by employees to conduct official business. The security of these devices is critical. If not properly managed, these work-related mobile devices can be exploited to gain access to the government's systems, networks, or data.

We found some areas for improvement and provided GSA's CIO with a set of recommendations. The CIO agreed with the recommendations and has put together a satisfactory corrective action plan to implement them.

While the report itself is not available to the public, we included a summary of it in our most recent Semiannual Report to the Congress, which is posted to our website and Oversight.gov. Additionally, an official copy of the restricted audit report has been provided to both majority and minority staff members of the Subcommittee for use in their official oversight work.

Conclusion

This concludes my overview of these three reports. My staff and I appreciate the Subcommittee's interest in our technology-related audit work.