GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

April 8, 2020

The Honorable Gerald E. Connolly
Chairman
Subcommittee on Government Operations
Committee on Oversight and Reform
House of Representatives

Dear Chairman Connolly:

On March 4, 2020, the Subcommittee on Government Operations held a hearing entitled, “Making IT a Priority for the Federal Government.” The attachment contains my response to the questions for the record following my testimony at this hearing. If you have any questions regarding these responses, please contact me at (202) 512-4456 or HarrisCC@gao.gov.

Sincerely yours,

Carol C. Harris
Director
Information Technology Acquisition Management Issues

Enclosure

cc: The Honorable Jody Hice, Ranking Member
Subcommittee on Government Operations, Committee on Oversight and Reform

Questions for Ms. Harris
Director, Information Technology and Cybersecurity, Government Accountability Office
Questions from Chairman Gerald E. Connolly

March 4, 2020, Hearing: "Making IT a Priority for the Federal Government."

1. **GAO has reported several times on agencies' telecommunications transition planning efforts. Compared to previous transitions, what improvements are agencies implementing in their planning efforts for the transition to Enterprise Infrastructure Solutions (EIS)? What are agencies not doing?**

   In general, the findings from our most recent review of selected agencies' planning efforts for the transition to EIS are consistent with our previous reviews of agencies' telecommunications transition planning efforts.[1] Agencies continue to make mixed progress in implementing the established planning practices that we have previously identified that can help agencies successfully transition their telecommunications services to new contracts. In all of our reviews, we have found that agencies have generally taken steps to implement certain activities associated with the practices. However, none of the agencies we reviewed had fully implemented all of the practices. We have seen that again as part of our most recent review of agencies' transition planning efforts.

   For example, while each of the five selected agencies in our most recent review had established inventories of their telecommunications assets and services, two of these agencies had only identified the assets and services that were associated with contracts managed by GSA. These two agencies did not identify their telecommunications assets and services associated with commercial contracts not managed by GSA.

   However, it is vital that agencies think about this transition as an opportunity for change and plan for it as such. Rather than focusing only on transitioning their services that are on current GSA contracts, agencies should be thinking about all of the services they currently use—including ones from other sources—and strategically planning how they can optimize their services or share them across the agency.

2. **You have stated that most of the agencies you looked at are upgrading or transforming services as part of their transitions. What does that entail?**

   There is no standard definition for what it means to upgrade or transform a service and, for our most recent review, we did not ask agencies for specific details on what services they are upgrading or transforming. However, several agencies told us that they plan to move voice services to internet-based options, improve cybersecurity, implement cloud computing services, or make other changes related to network services.[2]

[1] GAO, *Telecommunications: Agencies Should Fully Implement Established Transition Planning Practices to Help Reduce Risk of Costly Delays*, GAO-20-155 (Washington, D.C.: Apr. 7, 2020).

[2] Cloud computing is a means for enabling on-demand access to shared pools of configurable computing resources—such as networks and services—that can be rapidly provisioned and released.

3. **In the new eMarketplace, what are the potential consequences if the government procures goods that have supply chain vulnerabilities?**

   The National Institute of Standards and Technology (NIST) has identified several potential consequences related to procuring goods that have supply chain vulnerabilities, which may include goods procured in the eMarketplace. In its Special Publication 800-161, NIST identifies consequences such as the insertion of counterfeit goods into the supply chain; unauthorized production of goods; tampering of goods; theft of goods; and insertion of malicious software and hardware (e.g., GPS tracking devices and computer chips) into goods. For example, an adversary may have the power to insert malicious functionality into goods. Further, it may take years for a vulnerability stemming from the supply chain to be exploited or discovered.

4. **GAO has spent time analyzing agencies' abilities to vet and examine supply chain risks in their existing purchase processes. Do most individual agencies have plans or capacity to resolve supply-chain concerns for micro-purchases?**

   We currently have an ongoing review which includes work intended to address this question. The work we have under way is examining federal agencies' information and communications technology (ICT) supply chain risk management (SCRM) practices. Specifically, we are determining the extent to which 23 civilian agencies[3] have implemented practices for their non-national security systems[4] that are foundational for an organization-wide approach to ICT SCRM, for any purchase threshold. Foundational practices include establishing executive oversight for ICT SCRM activities; developing an agency-wide ICT SCRM strategy; and establishing an approach to identify and document agency ICT supply chain(s). Implementing these foundational practices can assist agencies in planning or having the capacity to manage supply chain risks. We plan to issue a report on the results of our review in late summer 2020.

[3] We are looking at the 23 civilian *Chief Financial Officers Act of 1990* agencies, which include the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development.

[4] According to the *Federal Information Security Modernization Act of 2014*, the term "national security system" is defined as 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, the function or use of which: involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapons system, is critical to the direct fulfillment of military or intelligence missions (with the exception of routine administrative of business systems), or stores, processes or communicates classified information. Systems that meet none of the above criteria are considered non-national security systems.