GAO@100 U.S. GOVERNMENT ACCOUNTABILITY OFFICE
A Century of Non-Partisan Fact-Based Work

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

May 14, 2021

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

FITARA 11.0 Hearing: Responses to Questions for the Record

Dear Chairman Connolly:

Thank you for the opportunity to testify before the Subcommittee on April 16, 2021, to discuss federal agencies' efforts to implement FITARA. We also appreciate the opportunity to provide the Subcommittee with additional information in response to questions for the record. Our responses can be found in the enclosure to this letter.

Please contact me with any further questions.

Sincerely yours,

Kevin C. Walsh
Director, Information Technology and Cybersecurity

Enclosure

cc: The Honorable Jody Hice, Ranking Member
Subcommittee on Government Operations

Enclosure

Post-Hearing Questions for the Record Submitted to Mr. Kevin Walsh
From Chairman Gerald E. Connolly
"Agency compliance with the Federal Information Technology Acquisition Reform Act (FITARA)"
April 16, 2021

1. **Are there any particular changes you would recommend that Congress consider as part of Federal Information Security Management Act reform efforts and for possible inclusion in a future Federal Information Technology Acquisition Reform Act (FITARA) scorecard?**

   GAO Response: At this time, we do not have any recommended changes to offer regarding Federal Information Security Management Act (FISMA) reform efforts and the FITARA scorecard. However, we are currently conducting our periodic evaluation of agencies' implementation of FISMA. The results of this work should further inform Congress on the effectiveness of FISMA and provide additional insights regarding improvements that could be made. We anticipate issuing the results of our work by the end of calendar year 2021.

2. **Why are supply chain risk management practices particularly important to information and communications technology?**

   GAO Response: The implementation of information and communications technology (ICT) supply chain risk management (SCRM) is essential for decreasing federal agencies' vulnerability to malicious actors that could exploit the ICT products and services (e.g. computing systems, software, and networks). Federal agencies face numerous ITC supply chain risks, including threats posed by counterfeiters who may exploit vulnerabilities in the supply chain and, thus, compromise the confidentiality, integrity, or availability of organizations' systems and the information they contain. Supply chain risk management practices offer an approach to managing cybersecurity risk and protecting organizations' critical information assets. Such practices specify control activities that organizations can use to provide additional supply chain protections, such as conducting due diligence reviews of suppliers and implementing procedures that help protect against supply chain threats throughout the system development life cycle.

   As highlighted in our December 2020 report, few of the 23 civilian Chief Financial Officers Act agencies had implemented seven selected foundational practices for managing information and communications technology (ICT) supply chain risks.[1] As a result, we made a total of 145 recommendations calling for agencies to, among other things, identify how the agency intends to assess, respond to, and monitor ICT supply chain risks across the life cycle of ICT products and services.

3. **The Government Accountability Office has stressed, since 2019, that the Office of Management and Budget and other covered federal agencies need to more fully implement FITARA guidelines. Can you please elaborate on what these agencies need to focus on?**

[1]GAO, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, GAO-21-171 (Washington, D.C.: Dec. 15, 2020).

GAO Response: As part of our March 2021 high-risk update, we reported that the Office of Management and Budget (OMB) and other federal agencies needed to focus on fully implementing critical requirements of federal IT acquisition reform legislation, such as FITARA, to better manage tens of billions of dollars in IT investments.[2] In particular, while agencies had fully implemented 65 percent of the roughly 1,400 recommendations that we have made since 2010, we noted that agencies still needed to implement 400 remaining recommendations. These included:

- our 2018 recommendations related to improving Chief Information Officer (CIO) authorities, as well as our 2016 recommendations on improving IT workforce planning practices;
- our 2019 recommendations related to improving cloud computing investment spending and savings data; and
- 11 priority recommendations for agencies to, among other things, report all data center consolidation cost savings to OMB.

Lastly, we recommended that agencies should consider applying effective practices that may better position them to fully implement FITARA provisions and realize IT management improvements and cost savings. These practices include, among other things, obtaining support from senior leadership, performing application rationalization[3] activities, and developing policies that explain how CIO authorities are to be carried out.

4. **If the subcommittee were to add a metric to the next FITARA scorecard involving the 21st Century IDEA Act (Public Law No: 115-336), what type of metric (and associated data) would allow us to better understand the effectiveness of an agency's implementation of this law?**

   GAO Response: We do not have any completed work related to the 21st Century Integrated Digital Experience Act (IDEA).[4] IDEA aims to improve the digital experience for government customers and reinforces existing requirements for federal public websites. However, we have observed that there are limited data publicly available regarding the implementation of IDEA that could be used for measuring its effectiveness. For example, https://digitaldashboard.gov/ is a test website that publishes disaggregated information on compliance and conformance metrics regarding the requirements for federal websites. However, the website requires a federal government employee account to access data. In addition, as of May 2021, no method exists to download or export the information provided on the website. Without the ability to analyze the data, we are not positioned to offer suggestions regarding the type of specific implementation metric that could be included on the scorecard.

5. **Now that the Software Licensing metric has been retired, what are the next steps the Subcommittee should consider to ensure agencies are effectively using software license inventories to make cost-effective decisions?**

---

[2]GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[3]Application rationalization is a process by which an agency streamlines its portfolio of software applications with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership.

[4]21st Century Integrated Digital Experience Act, Pub. L. No. 115-336, 132 Stat. 5025 (Dec. 20, 2018).

GAO Response: While continued oversight of agencies' efforts is essential, we have not yet conducted work that would offer insights regarding the next steps for ensuring agencies' effective use of software license inventories to make cost-effective decisions. However, our planned work to evaluate the most widely used software licenses in the federal government may better inform the Subcommittee.

As we reported in 2014, inadequate implementation of leading practices (including the establishment of software license inventories) resulted in agencies' inability to analyze software license data to more cost-effectively buy and maintain software licenses, and ascertain the software applications most widely used across the federal government.[5] Consequently, while some agencies were able to identify millions in savings for software through ad hoc processes, there was the potential for even greater savings and additional opportunities to reduce software license spending and duplication than what agencies had reported.

6. **When evaluating agencies' transition to the Enterprise Infrastructure Solutions program, are there ways to measure more than just the percentage of the transition, like how agencies might use this transition as an opportunity to modernize their networks?**

GAO Response: Agencies' transition to the Enterprise Infrastructure Solutions (EIS) program is currently measured by more ways than just the percentage of the transition. Specifically, the General Services Administration's (GSA) EIS Transition Progress Tracking Report includes data elements such as the number of fair opportunity solicitations needed and task orders awarded.[6]

Our work to date has not specifically assessed how agencies might use this transition as an opportunity to modernize their networks. However, during our prior review of agencies' telecommunications transition planning practices, we noted that federal agencies are using the transition off prior telecommunications contracts as an opportunity to modernize.[7] Specifically, our April 2020 review found that 15 agencies did not plan to implement a primary like-for-like transition. Rather, these agencies planned to upgrade or transform services other than those that GSA and the telecommunications contractors planned to discontinue. For example, as part of upgrading or transforming services, an agency could replace expiring services with alternative or advanced technology applications and solutions, such as implementing cloud computing services.[8]

[5]GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide,* GAO-14-413 (Washington, D.C.: May 22, 2014)

[6]GSA Transition Coordination Center, *EIS Transition Progress Tracking Report Dashboard for the period ending February 28, 2021* (Mar. 29, 2021).

[7]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).

[8]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.