August 30, 2022

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

Federal Information Technology Acquisition Reform Act (FITARA) Scorecard 14.0 Hearing: Responses to Questions for the Record

Dear Chairman Connolly:

Thank you for the opportunity to testify before the Subcommittee on July 28, 2022, to discuss 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 enclosures to this letter.

If you have any questions, please contact me at (202) 512-4456 or HarrisCC@gao.gov.

Sincerely yours,

Carol C. Harris
Director, Information Technology and Cybersecurity

Enclosures - 2

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

Questions for Ms. Carol C. Harris
Director, Information Technology and Cybersecurity
Government Accountability Office

Questions from Chairman Gerald E. Connolly
Subcommittee on Government Operations

July 28, 2022, Hearing: "FITARA 14.0"

---

1. **What are some of the most common challenges agencies encounter when they seek to establish a Modernizing Government Technology Act working capital fund?**

   GAO Response: We have not reviewed challenges agencies encounter when seeking to establish a Modernizing Government Technology Act (MGT act) working capital fund (WCF).[1] However, agencies have provided reasons for not establishing an MGT act WCF in the letters used to determine their scorecard grades.[2] These reasons include, but are not limited to, the existence of an established agency fund already in use or the lack of authority to transfer appropriated funds into a new WCF. For example, three agencies have existing access to funds that can be used for the purposes outlined in the MGT act and, as a result, do not plan to set up a MGT act WCF. In contrast, three other agencies have indicated that the agency does not have the authority to transfer funds into an MGT act WCF.

2. **Has the Government Accountability Office (GAO) published a report with multi-cloud strategy implementation recommendations for agencies, and if not, is the planning to develop a report in the future?**

   GAO Response: We have not published a report with multi-cloud strategy implementation recommendations for agencies. However, we have ongoing work evaluating the implementation of federal cloud strategies and security practices that is anticipated to be published in 2023. Upon request, we can discuss the scope and methodology of this work with the Subcommittee.

3. **Has the GAO published a report that assesses how effective a single cloud stack solution compares to a multi-cloud environment, and if not, is the Office planning to develop a report in the future?**

   GAO Response: We have not published a report that assessed the effectiveness of a single cloud stack solution compared to a multi-cloud environment. We discuss our ongoing related cloud work in the preceding response.

---

[1]The provisions commonly referred to as the *Modernizing Government Technology Act* establish working capital funds that allow agencies to use available amounts for purposes including IT modernization to enhance cybersecurity initiatives. *Modernizing Government Technology Act* provisions of the *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, div. A, title X, subtitle G, § 1077, 131 Stat. 1586, 1587 (2017).

[2]The Subcommittee receives letters from agencies regarding their efforts to establish a Modernizing Government Technology Act (MGT act) working capital fund. These letters respond to a series of questions asked by the Subcommittee and are the basis of the MGT act grade on the scorecard.

4. **Should executive agencies prioritize the acquisition of software that is cloud neutral? For the purposes of this question, cloud neutral means, software that can run equally efficiency on a variety of cloud providers servers without exorbitant migration costs.**

   GAO Response: We have not completed work related to whether agencies should prioritize the acquisition of software that is cloud neutral.

5. **As executive agencies continue to modernize federal IT systems and determine whether to utilize multi-cloud solutions, are there risks of increased cost, complexity, and security associated with a mandatory multi-cloud approach?**

   GAO Response: We do not have completed work that evaluates the risks, complexity, and security associated with a mandatory multi-cloud approach.

Enclosure II

<p align="center">**Questions for Ms. Carol C. Harris**
Director, Information Technology and Cybersecurity
Government Accountability Office

Questions from Ranking Member Jody Hice
Subcommittee on Government Operations

July 28, 2022, Hearing: "FITARA 14.0"</p>

1. **The description accompanying the Scorecard category titled "Enhanced Transparency and Improved Risk Management" says, "FITARA requires OMB to publicize detailed information on federal IT investments and requires agency CIOs to categorize their major IT investments by risk."**

    a. **What is the definition of "risk" and a "major IT investment" in this category?**

    b. **Do all agencies have the same definitions of "risk" and "major IT investment"?**

GAO Response: Risk and major IT investment for this category are defined based on Office of Management and Budget (OMB)'s guidance, which is applicable to all executive agencies.[1] Specifically for this category:

- **Risk** is defined by the Chief Information Officer (CIO). OMB's guidance states that the CIO should rate each investment's risk based on the CIO's best judgement of the investment's current level of risk in terms of its ability to accomplish its goals (per 40 U.S.C. § 11315 (c)(2)).

    The agency CIO is expected to rate each investment using a five-point scale (low risk, moderately low risk, medium risk, moderately high risk, and high risk). OMB's guidance notes that the CIO's evaluation of risk could be informed by the following list of factors: risk management, requirements/outcomes management, contractor oversight, performance, human capital, and other factors the CIO deems important to forecasting the investment's success.[2]

- **A major IT investment** is one requiring special agency management attention. According to OMB guidance, an IT investment is major if it is so designated by either the agency responsible for the investment or by OMB. Further, agencies must consult with OMB regarding which investments are considered major.

    When determining whether an investment should be designated as major, OMB's guidance notes that agencies should consider any relevant factors. These factors may include whether the investment requires special management attention because of its importance to an agency's mission or its implications for agency programs or policies. Factors may also include whether it is designated as a major IT investment in the previous budget submission, has a high annual cost (e.g., the total requested amount exceeds $10 million) or high projected total lifecycle cost. Additional factors could be whether the investment has

[1]The Office of Management and Budget publishes guidance to executive agencies on https://www.whitehouse.gov.

[2]Office of Management and Budget, *FY22 IT Budget – Capital Planning Guidance* (Nov. 16, 2020).

been designated as a high risk by the agency CIO, involves a high value asset, and has a high-visibility profile with agency executive leadership, congressional leadership, and/or the public.[3]

2. **According to the CIO Authority metric in the Scorecard, two agency CIOs do not report to their agency head or deputy, and six agency CIOs have partial access.**

   a. **Why are agencies not adhering to CIO Authority recommendations made years ago in the FITARA law?**

   b. **Is it appropriate to expect all agencies to have CIOs report directly to the agency head or deputy?**

   GAO Response: We have not completed work that specifically identifies reasons the eight agencies are not adhering to the statutory requirements for the CIO to report directly to the agency head.[4] As we have previously reported, OMB's Federal Information Technology Acquisition Reform Act (FITARA)[5] implementation guidance recognizes the need for agencies to comply with the law and states that CIOs should report to the head of the agency, either the Secretary or Deputy Secretary serving on the Secretary's behalf.[6] OMB's guidance also addresses the requirement in instances where agencies have implemented legislation under which a CIO reports to a Chief Operating Officer or other management executive. Specifically, the guidance states that the CIO shall have direct access to the agency head, particular to programs that include information technology.

3. **Are there categories not included in the Scorecard that could or should be added to better measure the information technology and cybersecurity posture of federal agencies?**

   GAO Response: In our March 2022 response to questions for the record related to this Subcommittee's FITARA 13.0 hearing, we identified a variety of information technology and cybersecurity categories that could be added to future scorecards, including customer experience, supply chain and cybersecurity risks, IT modernization, and workforce planning. However, there is a lack of publicly available data to enable incorporating these categories into the scorecard. For example, we have previously noted that the cybersecurity metric could be expanded to incorporate tracking agencies' progress toward building an appropriately skilled workforce. However, at this time, we are not aware of any aggregated workforce data that could be incorporated into the scorecard.

---

[3]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, Circular A-11 (Aug. 6, 2021).

[4]44 U.S.C. § 3506(a)(2)(A).

[5]The provisions commonly referred to as the *Federal Information Technology Acquisition Reform Act* are in the *Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, div. A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014).

[6]GAO, *Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities,* GAO-18-93 (Washington, D.C.: Aug. 2, 2018). Office of Management and Budget, *Management and Oversight of Federal Information Technology*, Memorandum M-15-14 (Washington, D.C.: June 10, 2015).