GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

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

March 1, 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) 13.0 Hearing: Responses to Questions for the Record

Dear Chairman Connolly:

Thank you for the opportunity to testify before the Subcommittee on January 20, 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,

CCHarris

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

January 20, 2022, Hearing: "FITARA 13.0"

1. **Given the current methodology behind the Scorecard, can agencies artificially inflate their grades? Please describe specific tactics agencies might use to raise their grades on the Scorecard without making meaningful changes to their IT infrastructure. How might we change the Scorecard to reflect agencies' progress more accurately?**

   GAO Response: The scorecard's reliance on agency-reported data allows for possible scenarios where information provided could yield a higher grade on the scorecard. For example, the methodology for the risk management metric (which assesses the portion of an agency's major IT investments risk by dollars) illustrates one way an agency can positively impact its grade based on the data provided. The metric methodology most recently used rewards agencies that are reporting more risk, i.e. medium and moderately high or high risk investments, on the Office of Management and Budget's (OMB) IT Dashboard.[1] As such, an agency could raise its risk management grade by reporting a greater portion of its investments as having medium or high risk.

   Changing the scorecard to more accurately measure progress is possible with the availability of additional data. Such data would be available with the new IT Collect Application Programing Interface that agencies used for submitting their fiscal year 2023 IT investment data. For example, with this new tool agencies are able to indicate whether an IT project is adequately implementing incremental development (one of the scorecard categories) and to provide information regarding the frequency of release iterations. Upon request, we will continue to assist the Subcommittee as it considers other potential changes to the scorecard that may more accurately depict agencies' progress.

2. **The FITARA Scorecard grades agencies on cybersecurity by combining the annual Federal Information Security Modernization Act (FISMA) assessments conducted by their affiliated inspector general with the reporting metrics agencies are required to submit to the Office of Management and Budget (OMB) as part of their Cross-Agency Priority goals on cybersecurity. Is this a sufficient measure of agency IT cybersecurity posture? Why or why not?**

   GAO Response: The Subcommittee's biannual scorecards have served as an effective oversight tool in monitoring agencies' cybersecurity efforts. For an issue as complex and wide ranging as cybersecurity, using a few selected measures, no matter how sound they might be, cannot be expected to provide a detailed, comprehensive view into an agency's overall posture. Although the most recently used methodology (noted above) provides useful

[1] The IT Dashboard is a public website that discloses data on federal IT spending, including information on IT investments and data centers, among other things.

insight into agencies' progress, the Subcommittee could consider adding measures to achieve more comprehensive insight into this area. Specifically, the Subcommittee could consider the extent to which agencies are mitigating global supply chain risks and improving the implementation of government-wide cybersecurity initiatives.

3. **As we look to update the FITARA cybersecurity metric, what are ways Congress can quantify and continuously monitor agency cybersecurity risk?**

GAO Response: Congress could quantify and continuously monitor agency cybersecurity risk by expanding the cybersecurity grade to include the extent to which GAO's cybersecurity recommendations are implemented. In our March 2021 high risk update, we reported that the federal government needs to move with greater urgency to improve the nation's cybersecurity as the country faces grave and rapidly evolving threats.[2] We reiterated the need for the federal government to take specific actions to address four major cybersecurity challenges: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[3] Our work evaluating progress toward addressing these four major cybersecurity challenges includes monitoring and reporting on agencies' progress in implementing about 3,700 recommendations aimed at remedying cybersecurity shortcomings. Agencies' progress in implementing these recommendations could be leveraged by the Subcommittee to quantify and monitor agency cybersecurity risk.

The Subcommittee may also consider the potential incorporation of a scorecard metric based on federal initiatives aimed at monitoring agency cybersecurity risk. For example, the Department of Homeland Security's continuous diagnostics and mitigation (CDM) program is intended to support government-wide and agency-specific efforts to provide adequate, risk-based, and cost-effective cybersecurity. Under this program, the Cybersecurity and Infrastructure Security Agency manages a federal dashboard that summarizes information about the security of agencies' networks, including a risk score based on data collected by agencies' CDM tools.[4] However, we do not know to what extent scores are publicly available. Further, as we reported in August 2020, poor data quality diminished the usefulness of those risk scores.[5]

[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] These specific actions are (1) develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace; (2) mitigate global supply chain risks; (3) address cybersecurity workforce management challenges; (4) ensure the security of emerging technologies; (5) improve implementation of government-wide cybersecurity initiatives; (6) address weaknesses in federal agency information security programs; (7) enhance the federal response to cyber incidents targeting federal systems; (8) strengthen the federal role in protecting the cybersecurity of critical infrastructure; (9) improve federal efforts to protect privacy and sensitive data; and (10) appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent. See GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[4] Such data includes unauthorized hardware, configuration settings, and vulnerabilities.

[5] GAO, *Cybersecurity: DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program*, GAO-20-598 (Washington, D.C.: Aug. 18, 2020).

Another possible approach would be to monitor actions taken to implement the May 2021 Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*.[6] The EO includes required actions intended to help modernize federal government cybersecurity, enhance software supply chain security, and improve detection of vulnerabilities and incidents, among other things. We have ongoing and planned work related to these topic areas. The results of this work may further inform the Subcommittee on ways to further monitor agency cybersecurity risk.

4. **Can Congress implement effective updates to the Scorecard's cybersecurity metric with public data? If not, how can the Subcommittee protect sensitive agency information while holding agencies accountable for cybersecurity?**

GAO Response: As noted in our April 2021 testimony before the Subcommittee, the use of nonpublic data on agencies' cybersecurity activities would expose agency vulnerabilities to potential attacks.[7] However, as discussed by witnesses during the Subcommittee's January 20, 2022 hearing, there is a possibility of handling sensitive information that may allow for the use of nonpublic data in assessing agencies' cybersecurity posture without vulnerable exposure. Should the Subcommittee wish to pursue the use of nonpublic data for monitoring agencies' cybersecurity, we offer our continued assistance in discussing potential methodologies and associated data sources.

5. **In June 2019, the Government Accountability Office (GAO) published a report analyzing IT modernization plans for the most critical legacy systems in our federal government. GAO found that of the ten agencies responsible for these legacy systems, only two had adequate plans to modernize their systems and three had no plans to modernize at all.**

Nearly three years after the release of GAO's report, eight of the ten agencies have yet to produce workable modernization plans. What impact does poor IT modernization planning have on the federal government's IT investments and its ability to spend taxpayer dollars effectively?

GAO Response: As highlighted in our June 2019 report, there is a negative impact that poor IT modernization planning can have on the federal government's IT investments and its ability to spend taxpayer dollars effectively.[8] Specifically, agencies that lack complete legacy system modernization plans will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure could be particularly detrimental for systems most in need of modernization. This is because prolonging the lifespan of these increasingly vulnerable systems exposes the agency and system clients to security threats and performance issues.

[6] Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

[7] U.S. Congress, House of Representatives, Subcommittee on Government Operations of the Committee on Oversight and Reform. *Agency Compliance with the Federal Information Technology Acquisition Reform Act (FITARA)*, 117th Cong., 1st sess., 2021, 117-14.

[8] GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471, (Washington, D.C.: June 11, 2019).

Federal IT legacy systems are becoming increasingly obsolete and can be more costly to maintain, more exposed to cybersecurity risks, and less effective in meeting their intended purpose.[9] Further, federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems; upgrading underlying infrastructure; and investing in high quality, lower cost service delivery technology.

6. **How might the Subcommittee incorporate IT modernization and workforce planning into the FITARA Scorecard?**

GAO Response: As we have reported in the past, there are specific attributes related to critical federal legacy systems and key workforce planning activities. If tracked and reported, some portion of these attributes could be considered for developing a scorecard metric related to IT modernization and workforce planning. For example,

- In June 2019, we identified the 10 most critical federal legacy systems in need of modernization at the 24 Chief Financial Officer (CFO) Act agencies.[10] We assessed these systems against attributes for determining systems' obsolescence and their need for modernization, including the system's hardware status, use of legacy programming languages, and criticality and risk (as identified by the agency).

- In October 2019, we assessed the 24 CFO Act agencies' implementation of eight key workforce planning activities.[11] These activities include developing competency and staffing requirements, assessing gaps in competencies and staffing, implementing activities that address gaps, and monitoring agencies' progress in addressing competency gaps.

Upon request, we can work with the Subcommittee to identify potential data sources that may enable the development of a metric related to agencies' IT modernization and workforce planning efforts.

7. **Government-owned and operated data centers can use excessive energy if they are not optimized for efficiency. Data center energy consumption represents 1-2% of global electricity use. Under OMB guidance, agencies are generally required to have advanced energy metering at federal data centers. Yet, according to work conducted by GAO, only 22% of federal data centers have electricity metering. Is GAO able to get an accurate picture of energy use at federal data centers?**

GAO response: During 2021, we analyzed the extent to which federal agencies have information on data center energy usage and determined that a complete and accurate picture of energy use at federal data centers was not possible at that time.[12] This was

[9] The Modernizing Government Technology (MGT) Act defines a legacy IT system as a system that is outdated or obsolete. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1587 (2017).

[10] GAO-19-471.

[11] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, GAO-20-129. (Washington, D.C.: Oct. 30, 2019).

[12] Due to the results of our analysis, we terminated our work and have not publicly published these observations.

because roughly three-fourths of the federal data centers did not have a means for measuring energy usage (i.e., electricity meters do not exist for these centers).

8. **Consolidating and optimizing data centers and moving to the cloud results in savings and more efficient and nimbler IT. How can this Subcommittee ensure agencies continue to optimize their data centers and transition to the cloud?**

GAO Response: One way the Subcommittee can ensure agencies continue to optimize their data centers and transition to the cloud would be through encouraging OMB to implement several recommendations we have made that specifically address both of these important areas. With respect to data centers, we noted during the Subcommittee's January 20, 2022, hearing that agencies have closed roughly 6,800 data centers and achieved $6.6 billion in savings since 2010. However, in March 2021 we reported that revisions to data center guidance made in 2019 resulted in a metric that no longer reported on actual server utilization, an aspect of optimization.[13] Accordingly, we recommended that OMB reexamine its data center optimization initiative guidance regarding how to measure server utilization and revise it to better and more consistently address server efficiency.

We also reported that agencies have made progress in implementing cloud services and, in doing so, have saved hundreds of millions of dollars and realized notable benefits. According to OMB, cloud services offer agencies a number of benefits, including reduced IT procurement and operating cost, and increased efficiency and effectiveness in delivering services. However, in two separate 2019 reports, we determined that 1) agencies did not have sufficient mechanisms or approaches to track and report the savings data associated with cloud initiatives and 2) although federal agencies increased their use of FedRAMP (a required federal authorization program that provides a standardized approach to ensure that cloud services meet federal security requirements), they continued to authorize the use of cloud services that had not been approved by the program.[14] We therefore recommended that OMB 1) require agencies to report, at least on a quarterly basis, the savings and cost avoidances associated with cloud computing investments,[15] and 2) establish a process for monitoring and holding agencies accountable for authorizing cloud services through FedRAMP.

As of February 2022, OMB had not yet taken actions to fully implement these data center and cloud related recommendations.

[13] GAO, *Data Center Optimization: Agencies Report Progress and Billions Saved, but OMB Needs to Improve Its Utilization Guidance,* GAO-21-212 (Washington, D.C.: Mar. 4, 2021).

[14] GAO, *Cloud Computing Security: Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed,* GAO-20-126 (Washington, D.C.: Dec. 12, 2019) and *Cloud Computing: Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked,* GAO-19-58 (Washington, D.C.: Apr. 4, 2019).

[15] While OMB requires agencies to report savings, the reporting instructions do not specifically require the identification and reporting of cloud savings as a separate category of cost savings and avoidance.

9. **How can the FITARA Scorecard accurately measure agency adoption of user- and customer-centric design and implementation processes?**

   GAO Response: To measure agency adoption of user- and customer-centric design and implementation processes, the Subcommittee can consider the potential incorporation of a metric based on federal initiatives aimed at improving customer experience. Examples of these initiatives include:

   - **The 21st Century Integrated Digital Experience Act (21st Century IDEA).**[16] On December 20, 2018, the President signed 21st Century IDEA into law. Under 21st Century IDEA, agencies must meet eight specific requirements for modernizing their websites. Among other things, agencies' new or redesigned websites, web-based forms, web applications, and digital services must be accessible to individuals with disabilities, designed around user needs with data-driven analysis (i.e. user-centered), and mobile friendly.

   - **Office of Management and Budget, *Circular No. A-11: Managing Customer Experience and Improving Service Delivery*.**[17] OMB guidance for implementing the federal government customer experience framework requires agencies to annually assess the customer experience capacity of their high-impact service providers, including whether they use human-centered design.[18]

   - **Executive Order (EO) 14058, *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government.***[19] This EO calls for several agency actions to improve the digital experience for their respective agencies' customers by modernizing agency websites and using human-centered design methodologies, among other things.

   As shared with the Subcommittee previously, at this point in time there is a lack of aggregated publicly available data on agencies' efforts toward implementing these initiatives. It should also be noted that certain requirements in OMB's customer experience guidance from Circular No. A-11 and the December 2021 EO 14058 apply to designated high-impact service providers, which do not span all the agencies included on the scorecard. We offer our assistance in further discussing how agency adoption of user- and customer-centric design and implementation processes could be included in the scorecard.

[16] 21st Century Integrated Digital Experience Act, Pub. L. No. 115-336, 132 Stat. 5025, 5026 (Dec. 20, 2018).

[17] Office of Management and Budget, *Circular No. A-11: Managing Customer Experience and Improving Service Delivery,* Section 280 (Washington D.C.: Aug. 6, 2021).

[18] OMB designates federal entities as high-impact service providers due to their large customer base or high impact on those serviced by the program. For fiscal year 2022, the 35 designated high-impact service providers spanned 17 federal agencies. Examples include the Department of State's Passport Services, the Department of Veterans Affairs Veterans Health Administration, and the Department of Agriculture's Farm Services Agency. The current list of high-impact service providers is available at https://www.performance.gov/cx.

[19] Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (Dec. 13, 2021).

10. In December 2021, GAO noted that the Technology Modernization Fund (TMF) sees a shortfall in the fees collected compared to its operating expenses. As of August 2021, operating expenses totaled $2.8 million compared to about $810,000 in fees collected. What impact might this have on the TMF's future?

GAO Response: At this time, we are not able to provide a clear picture regarding how the shortfall in the fees collected might impact the future of the TMF.[20] From the Fund's creation through fiscal year 2021, Congress appropriated $175 million for the TMF, from which 11 projects were awarded $89 million. OMB's 2018 TMF guidance directed agencies with approved projects to reimburse the amounts transferred from the fund and pay a fee, within 5 years of award. The General Services Administration (GSA) uses TMF appropriations to cover its operating expenses, and collects the fees required by the OMB guidance to offset these expenses. As we previously reported, in March 2021 the American Rescue Plan Act of 2021 appropriated an additional $1 billion to the TMF and on September 30, 2021 GSA announced the approval of seven new projects with awards totaling at least $311 million (one of the seven projects is classified; no award figure is publicly available).[21]

We reported in December 2019, and reiterated in December 2021, that the TMF operating expenses outpaced the fee collection intended to offset those expenses.[22] Specifically, the fund was able to offset only about 29 percent of the obligated operating costs as of August 31, 2021, and it is not clear when the TMF program office will fully recover future operating expenses incurred in fiscal year 2022 and beyond. Further, as of November 2021, the fee structures for reimbursing the TMF associated with the seven new projects remained unpublished, making it unclear how much in fees will be recovered from the September 2021 awards.

As a result, there remains risk that the planned fee collection for all awarded projects will fall short of covering the TMF's operating expenses. In our initial 2019 report, we concluded that this meant there would be fewer funds available to award to projects intended to improve the efficiency and effectiveness of government IT systems. We consequently recommended that OMB and GSA work together to develop and implement a plan to outline the actions needed to fully recover the TMF operating expenses in a timely manner. However, as we reported in December 2021, a plan had not been fully developed and decisions regarding fee rates and the funding model for GSA's TMF Program Management Office were not finalized.

[20] The provisions of the National Defense Authorization Act for Fiscal Year 2018 commonly referred to as the Modernizing Government Technology (MGT) Act, established the TMF, within the Department of the Treasury. 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, 131 Stat. 1283, 1586-94 (2017).

[21] American Rescue Plan Act of 2021 (ARPA), Pub. L. No 117-2, 135 Stat. 4, 80 (2021).

[22] GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects*, GAO-20-3 (Washington, D.C.: Dec. 12, 2019) and *Technology Modernization Fund: Implementation of Recommendations Can Improve Fee Collection and Proposal Cost Estimates,* GAO-22-105117 (Washington, D.C.: Dec. 10, 2021).

11. Has GAO reviewed the time it takes for agencies to receive their TMF funding after project award? If so, on average, how much time does it take for agencies to receive their funds?

GAO Response: We have not reviewed the time it takes for agencies to receive their TMF funding after project award. However, we have reported that agencies recommended for TMF funding are required to sign a written agreement documenting the purpose for which the funds will be used and the terms of repayment.[23] In addition, OMB guidelines state that projects are to receive incremental funding contingent on the successful execution of milestones outlined in the written agreement for the transfer of funds.[24]

We reported that, as of August 31, 2021, seven of the 11 approved projects had received the full transfer of awarded funds.[25] These seven projects were awarded funds between June 2018 and August 2019. Of the remaining four projects that were awarded funding between September 2019 and August 2021, three received at least one transfer of awarded funds. According to officials responsible for the fourth project, the funds have not yet been received after seven months because the project's start and completion dates were still being determined. Moreover, according to the most recent update to the TMF website dated December 29, 2021, the initial transfer is in process for six of the seven new awards announced in September 2021.[26]

12. Are there changes to the TMF process that GAO would recommend to help agencies get their funding more quickly?

GAO Response: GAO has made recommendations aimed at improving TMF processes. For example, in 2019 we recommended that GSA develop detailed guidance for the TMF project cost estimate template, including information on the data elements and the fields required to be completed.[27] In 2021, GSA took steps to update the template, however, actions remain to ensure that the template includes detailed guidance related to required data elements and fields that would help ensure the accuracy and completeness of the provided information. Accurate and complete proposals are especially important because, as we reported in December 2021, the majority of the awarded projects have yet to realize cost savings and a number of projects have delayed the dates by which they expect to realize their savings.[28]

Moreover, in our December 2021 report, we noted that approximately 85 percent of the initially approved projects narrowed their scopes and this led to reduced award amounts transferred to agencies. Specifically, as of August 31, 2021, six of the initial seven awarded

[23] GAO-22-105117.

[24] Office of Management and Budget, *Funding Guidelines for Agencies Receiving Disbursements from the Technology Modernization Fund* (Washington, D.C.: Dec. 31, 2020).

[25] GAO-22-105117.

[26] OMB provides information on the status of awarded projects on the Technology Modernization Fund's website at https://tmf.cio.gov/. On September 30, 2021, the General Services Administration announced the approval of seven new projects. The award status is not publicly available for one project because the project is classified.

[27] GAO-20-3.

[28] GAO-22-105117.

projects requested and received Technology Modernization Board approval of significant reductions to their approved scope, which in turn resulted in these projects requiring $46.92 million less in funding. Given the hundreds of millions of dollars remaining in the fund to address urgent IT modernization challenges, the post-award changes to past projects, and the delays in realizing savings, it is increasingly important that the quality of the documentation provided by applicant agencies be complete, accurate, and reliable.

Questions for Ms. Carol C. Harris

Director, Information Technology and Cybersecurity
Government Accountability Office

January 20, 2022, Hearing: "FITARA 13.0"

Questions from Rep. Jody Hice

1. **As the Subcommittee reviews the FITARA Scorecard and thinks about revisions to make it more useful, should the Data Center Optimization Initiative (DCOI) be removed or modified as a metric?**

   GAO Response: The current methodology for the data center metric has served its purpose in monitoring agencies' progress toward completion of Office of Management and Budget (OMB) established goals and can be removed from the scorecard. In November 2015 when the Subcommittee began issuing biannual scorecards as an oversight tool, 75 percent of the 24 agencies received an F or no grade for the data center metric. In contrast, for the December 2021 scorecard all agencies received A grades. Moreover, we noted during the Subcommittee's January 20, 2022, hearing that agencies have closed roughly 6,800 data centers and achieved $6.6 billion in savings since 2010.

2. **FITARA is generally credited for helping agencies bolster their IT posture in part because of this Subcommittee's comprehensive oversight of the law and Scorecard, evidenced by the fact that this is the 13th FITARA hearing we have held. Yet, since 1997, GAO to this day continues to identify federal IT security as a government-wide high-risk area.**

   a. **If 13 oversight hearings have not yet helped take federal IT off the GAO's high-risk list, what will it take?**

   b. **Do federal agencies treat these FITARA hearings as a check-the-box compliance exercise?**

   GAO Response: Congressional hearings are an important aspect of oversight aimed at improving cybersecurity. We are convinced that such hearings have brought focused attention on the need to improve cybersecurity.

   Nevertheless, GAO has specific criteria for determining removal of areas from our high-risk list. These criteria include leadership commitment, capacity (i.e., people and resources) to resolve the risk(s), a corrective action plan, monitoring, and demonstrated progress.[1] In our March 2021 update to our high-risk series, the status of these criteria for ensuring the cybersecurity of the nation had declined since our 2019 update. Our experience is that federal agencies do not treat the hearings as check-the-box compliance exercises. Rather, we have observed that agency officials take their preparations for the hearings seriously and

[1] Our March 2021 High Risk Update provides more details on these criteria; see 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).

that selected agencies devote time to calculating their own grades in advance of the scorecard release.

3. **The issuance of a December 2021 OMB guidance on "Federal Information Security and Privacy Management Requirements," along with the May 2021 Executive Order on "Improving the Nation's Cybersecurity," portends upcoming changes for agencies' FISMA reporting requirements.**

    a. **How should the guidance and directions in these documents be applied to the FITARA Scorecard's cyber metric?**

    b. **The forthcoming President's Management Agenda with new CAP Goals will also impact agency reported metrics. How is GAO preparing to adjust its information gathering and analysis to incorporate any new information into its preparation of future Scorecards, and what should the Subcommittee be paying attention to as the Administration rolls out new goals?**

    c. **Does GAO have any work planned to examine the FISMA reporting requirements in the context of direction provided from the above referenced documents and from any other guidance issued by the current Administration?**

GAO Response: We have a variety of work underway evaluating efforts to improve the nation's cybersecurity. The results of this work may better inform the Subcommittee with ways to incorporate government-wide initiatives, such as those outlined in OMB's December 2021 guidance and the May 2021 Executive Order (EO), into the scorecard. As noted above, the forthcoming President's Management Agenda and new cross-agency priority (CAP) goals may affect the methodology for the scorecard cybersecurity metric. As the Subcommittee makes its considerations, it should be noted that relevant data would need to be made publicly available to apply OMB's December 2021 guidance on federal information security and privacy requirements and the May 2021 EO to the scorecard.[2] One way this could be achieved would be through updated CAP goals that reflect the priorities cited in these documents. Before publicly publishing data, OMB would need to take into consideration the sensitivity of such information.

The Federal Information Security Modernization Act (FISMA) includes a provision for GAO to periodically report to Congress on implementation of the act.[3] As agreed with cognizant committees, we have chosen to issue such a report roughly every other year. Our current effort includes an evaluation of agencies' implementation of CAP goals. We anticipate issuing this report during this calendar year. We have not yet started planning the scope of

[2] Office of Management and Budget, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements M-22-05*, (Washington, D.C.: Dec. 6, 2021) and Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

[3] The Federal Information Security Modernization Act of 2014 (FISMA 2014), Pub. L. No. 113-283, 128. Stat. 3073, 3083 (2014). FISMA 2014 largely superseded the Federal Information Security Management Act of 2002 (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (2002). This act promotes the use of security tools to continuously monitor and diagnose an agency's cybersecurity posture and improve oversight of their information security programs.

our next periodic FISMA report, but will take into consideration any changes to reporting requirements or other guidance as appropriate.

4. In a December 2020 report on supply chain risk management, GAO notes,

> **[A]gencies face numerous ICT [information and communications technology] 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 an organization's systems and the information they contain.[4]**

This is what happened with the SolarWinds hack in 2020 when a third-party software supplier became an adversary's attack vector. Should the FITARA Scorecard include a metric specifically tied to supply chain risk management?

GAO Response: Given the continuing increase in cyberattacks as illustrated by the SolarWinds and Microsoft Exchange Server hacks, the Subcommittee could consider adding a metric related to supply chain risk management. Although federal agencies have taken steps to address IT supply chain deficiencies that we previously identified, this area continues to be a potential threat vector for malicious actors to target the federal government. For example,

- In 2018, we identified mitigating global supply chain risks as one of 10 critical actions needed for federal agencies to address major cybersecurity challenges.[5] We have also previously reported on risks to the IT supply chain, including those originating from foreign-manufactured equipment.

- In July 2017, we reported that the Department of State had relied on certain device manufacturers, software developers, and contractor support which had suppliers that were reported to be headquartered in a cyber-threat nation (e.g., China and Russia).[6]

- In December 2020 we reported that 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.[7] 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.

At the Subcommittee's request, we will provide assistance to help consider possible

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

[5] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[6] GAO, *State Department Telecommunications: Information on Vendors and Cyber-Threat Nations,* GAO-17-688R (Washington, D.C.: July 27, 2017).

[7] GAO-21-171.

methodologies and associated data sources that may be available for inclusion in the scorecard.

5. **Identifying, hiring, and retaining a cyber workforce is a constant challenge for both public and private sector, but federal agencies have unique challenges.**

   a. **How proactive are federal agencies in developing strategies to address their current workforce needs?**

   b. **Would an IT workforce category be a good addition to future Scorecard metrics?**

GAO Response: Our work on agencies' progress in implementing related statutory requirements and workforce planning practices may provide insight into potential ways the Subcommittee might develop a related metric for the scorecard.

- In June 2018 and March 2019, we reported on agencies' implementation of the Federal Cybersecurity Workforce Assessment Act of 2015.[8] The act is intended to address cybersecurity skills gaps within the executive branch of the federal government and requires federal agencies to take several actions related to cybersecurity workforce planning. Our reports noted that agencies have taken steps to address the act's requirements and made progress toward developing strategies to address shortages and skills gaps in their cybersecurity workforce.[9] However, not all agencies met the deadlines set forward by the act to address these gaps. We also have recommendations that remain to be addressed regarding meeting the act's requirements.

- In October 2019, we reported that agencies varied widely in their efforts to implement key IT workforce planning activities and had not made workforce planning a priority, despite laws and guidance which have called for them to do so for over 20 years.[10] Effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary skills, and abilities to execute a range of management functions that support agencies' missions and goals.[11] Until this occurs, agencies will likely not have the staff with the necessary knowledge, skills, and abilities to support their mission and goals.

[8] The act generally refers to the cybersecurity workforce as those positions requiring the performance of IT, cybersecurity, or other cyber-related job functions. The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted as part of the Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title III, sec. 303 (Dec. 18, 2015); 129 Stat. 2242, 2975-77.

[9] GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs,* GAO-19-144 (Washington, D.C.: Mar. 12, 2019) and *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions,* GAO-18-466 (Washington, D.C.: June 14, 2018).

[10] GAO, *Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities,* GAO-20-129 (Washington, D.C.: Oct. 30, 2019).

[11] GAO, *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps,* GAO-17-8 (Washington, D.C.: Nov. 30, 2016).

Given the importance of continued oversight in this area, the Subcommittee may consider ways it could hold agencies accountable for implementing statutory provisions and key IT workforce planning activities. For example, the cybersecurity metric could be expanded to incorporate tracking agencies' progress toward building an appropriately skilled workforce or whether agencies have a strategic plan in place related to training and retaining a cybersecurity workforce. However, at this time, we are not aware of any aggregated IT workforce data that could be incorporated into the scorecard and can work with the Subcommittee to consider other options that may be available.

6. **The problem of legacy federal IT systems is a frequent focus of this Subcommittee. Is it appropriate to devise metrics to specifically track progress updating or eliminating the most critical legacy systems?**

   GAO Response: We agree it would be appropriate to devise a metric that tracks progress toward updating or eliminating the most critical legacy systems. While we are not aware of data available that accurately measure such a topic, there are specific attributes related to critical federal legacy systems that, if tracked and reported, could potentially be considered for developing a scorecard metric. For example, in June 2019 we reported on government and industry best practices for the modernization of federal IT.[12] In this review, we identified that agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system. We also reported that most agencies in our review did not have complete plans to modernize these legacy systems.

   Upon request, we can work with the Subcommittee to identify potential data sources that may enable the development of a metric related to agencies' efforts to modernize or decommission their mission critical legacy IT systems.

7. **As described on its website, the IT Dashboard "shines light onto the performance and spending of IT investments across the Federal Government. If a project is over budget or behind schedule, you can see by how much money and time, and you can see the person responsible."[13] Should this, or some variation of on-time and on-budget data be included as a metric on the FITARA Scorecard?**

   GAO Response: The IT Dashboard includes cost and schedule data that could be considered by the Subcommittee as part of a metric on the scorecard. As we have previously reported, the IT Dashboard presents performance ratings for agencies using metrics that OMB has defined—cost, schedule, and Chief Information Officer evaluation. The IT Dashboard calculates these ratings by determining cost and schedule variances based on agency submitted data, such as planned versus actual costs or planned versus

[12] GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems,* GAO-19-471 (Washington, D.C.: June 11, 2019).

[13] IT Dashboard, *Frequently Asked Questions* (online at https://itdashboard.gov/drupal/frequently-asked-questions).

actual completion dates.[14] We offer our assistance in further exploring what potential variation could be used.

8. **The FITARA scorecard captures high-level agency-specific data. We understand that an agency's information often reflects several different components/bureaus – some of which may artificially inflate or deflate the overall score. Is it possible, and if so, is it advisable that we capture more granular details in a way that helps us understand which agency components are doing well and which ones are not?**

   GAO Response: Some of the data sources that support the scorecard include more granular data at the component/bureau level, making it potentially possible to capture those details on the scorecard. However, we would not advise doing so at this time. Based on our experience, it will be challenging enough to add new IT categories and gain agreement on these changes with the agencies. It may also take multiple iterations of selected areas to get the scoring methodologies to most accurately reflect reality. We would advise exploring options for including more granular details at component/bureau level once the updates to the scorecard categories and corresponding methodologies have stabilized. In the interim, we offer our assistance to work with the Subcommittee to provide key component/bureau level details where available to help support its oversight work.

9. **The Subcommittee continues to consider ways to advance the implementation of enhanced customer experience across the federal government, particularly the digital experience as espoused in the 21st Century IDEA, as well as principles of Executive Order 14058. An important aspect of this consideration is development of metrics associated with the various requirements, including website modernization, forms modernization, and related requirements.**

   a. **What are your thoughts on metrics associated with customer experience and implementation of 21st Century IDEA, and how could those be applied to the FITARA scorecard?**

   b. **Are you aware of any agencies that have proactively taken steps to track their compliance with the requirements of 21st Century IDEA? If so, what have they done?**

   GAO Response: As shared with the Subcommittee previously, at this point in time there is a lack of aggregated publicly available data on agencies' efforts toward implementing the 21st Century Integrated Digital Experience Act (IDEA).[15] It should also be noted that certain requirements in the December 2021 EO 14058 apply to designated high-impact service providers, which do not span all the agencies included on the scorecard.[16] We offer our assistance to further discuss the potential of developing a scorecard metric related to customer experience and 21st Century IDEA. We have not performed work related to

[14] GAO*, IT Dashboard: Agencies Need to Fully Consider Risks When Rating Their Major Investments,* GAO-16-494 (Washington, D.C.: June 2, 2016).

[15] 21st Century Integrated Digital Experience Act, Pub. L. No. 115-336, 132 Stat. 5025 (Dec. 20, 2018).

[16] Executive Order 14058, *Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government* (Dec. 13, 2021).

agencies' efforts to implement 21st Century IDEA. Accordingly, we do not know to what extent agencies have or have not been proactive in meeting the act's requirements or reporting on their compliance. Upon request, we could conduct a study that may provide Congress with additional insights into this area.