

**Congress of the United States**  
**House of Representatives**

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051  
MINORITY (202) 225-5074  
<https://oversight.house.gov>

September 27, 2022

Ms. Clare Martorana  
Federal Chief Information Officer  
Office of Management and Budget  
725 17th Street, N.W.  
Washington, D.C. 20506

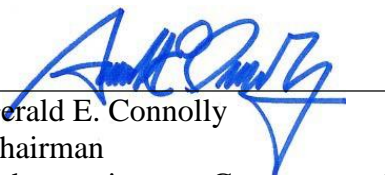
Dear Ms. Martorana:

Enclosed are post-hearing questions that have been directed to you and submitted to the official record for the hearing that was held on Friday, September 16, 2022, entitled "Project Federal Information Technology: Make IT Work."

To ensure a complete hearing record, please return your written response to the Subcommittee on or before October 11, 2022, including each question in full as well as the name of the Member. Your response should be addressed to the Committee office at 2157 Rayburn House Office Building, Washington, D.C. 20515. Please also send an electronic version of your response by email to Amy Stratton, Deputy Chief Clerk, at [Amy.Stratton@mail.house.gov](mailto:Amy.Stratton@mail.house.gov).

Thank you for your prompt attention to this request. If you need additional information or have other questions, please contact Elisa LaNier, Chief Clerk, at (202) 225-5051.

Sincerely,



Gerald E. Connolly  
Chairman  
Subcommittee on Government Operations

Enclosure

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

**Questions for Ms. Clare Martorana**  
Federal Chief Information Officer

**Questions from Chairman Gerald E. Connolly**  
Subcommittee on Government Operations

September 16, 2022, Hearing: “Project Federal Information Technology: Make IT Work”

---

1. **The Federal Information Technology Acquisition Reform Act (FITARA) Scorecard uses data to assess agencies that are both publicly available and consistent across agencies. That way, these metrics can accurately assess data in a way that is safe, understandable, and transparent to the public.**
  - a. **How can the government most accurately measure and publicly communicate cybersecurity preparedness while ensuring agencies do not become targets of bad actors?**

**Answer:** The prevention, detection, assessment, and remediation of cyber incidents is a top priority for this Administration. Beginning with Presidential Executive Order 14028, *Improving the Nation’s Cybersecurity* (EO 14028), this Administration has publicly communicated both strategy and direction on cybersecurity preparedness. EO 14028 sets forth the strategic direction for the Federal enterprise to invest in technology, people, and doctrine to modernize cyber defenses over the next few years and established standards and requirements that all Federal information systems should meet or exceed. Additionally, the Administration has published two National Security Memoranda addressing cybersecurity preparedness.<sup>1</sup>

OMB publishes policy and guidance as appropriate in support of the Executive Order. During this Administration, OMB has issued five memoranda to agencies to implement EO 14028. They include memos on critical software,<sup>2</sup> logging,<sup>3</sup> endpoint detection and response,<sup>4</sup> zero trust strategy,<sup>5</sup> and ensuring use of securely developed software.<sup>6</sup> Additionally, OMB publishes annual Federal Information Security Modernization Act (FISMA) guidance<sup>7</sup> in accordance with FISMA 2014 and coordinates with the Cybersecurity and Infrastructure Security Agency (CISA) to issue both the CIO<sup>8</sup> and Inspector General (IG)<sup>9</sup> FISMA metrics. Further, CISA publishes Emergency Directives and Binding Operational Directives as necessary to mitigate and reduce

---

<sup>1</sup> Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems (National Security Memorandum/NSM-8) and National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (National security Memorandum/NSM-10).

<sup>2</sup> M-21-30, *Protecting Critical Software Through Enhanced Security Measures*

<sup>3</sup> M-21-31, *Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents*

<sup>4</sup> M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*

<sup>5</sup> M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*

<sup>6</sup> M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

<sup>7</sup> The latest FISMA guidance is M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.

<sup>8</sup> <https://www.cisa.gov/sites/default/files/publications/FY22%20FISMA%20CIO%20Metrics.pdf>

<sup>9</sup> <https://www.cisa.gov/sites/default/files/publications/FY%202022%20Core%20IG%20FISMA%20Metrics%20Evaluation%20Guide%20%2805-12-22%29.pdf>

vulnerabilities.<sup>10</sup> The Executive Order, OMB policy and guidance, the CIO and IG FISMA metrics, and directives published by CISA are all publicly available. These are only a few examples of how the Federal Government publicly communicates its priorities for cybersecurity preparedness within and across Federal agencies, and shares its approach to measuring agency cybersecurity performance.

Finally, as described in my testimony, OMB currently has an effort underway to update what information OMB and the CIO Council publish about agency cybersecurity performance in order to provide Congress and the public with an accurate picture of how agencies are performing on key Federal cybersecurity indicators. Because cybersecurity datasets can be complex, our goal when releasing cybersecurity data is to focus agencies and the public on an accurate picture of the security of Federal systems and the areas where investments need to be made. We must also balance transparency with security concerns, and ensure that these potentially sensitive datasets are shared in a way that does not focus adversary attention on potential gaps to exploit.

**2. The Modernizing Government Technology Act authorized agencies to create a working capital fund. Unfortunately, not all agencies have implemented this funding mechanism that allows for greater planning and multi-year investment commitments.**

**a. What alternative funding streams would you recommend to agencies to ensure they have the necessary capital to implement information technology (IT) modernization changes?**

**Answer:** Large IT modernization projects typically require on-demand flexibility and variable funding levels from year to year. The annual appropriations process can create risk and uncertainty in IT projects and other funding streams may provide alternative approaches to funding IT investments. OMB has historically been supportive of agencies that seek to use the authorities granted by the Modernizing Government Technology (MGT) Act to establish and use a Working Capital Fund (WCF). Outside of the MGT WCF, some agencies already have the authority to use multi-year appropriations accounts to fund IT projects or accounts such as a Non-recurring Expense Fund (NEF) that enable the collection of unused resources to fund capital investments.

**3. The Federal Chief Information Officer (CIO) Information Technology Operating Plan, the Cybersecurity Executive Order, and Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements all prioritize cybersecurity for agency CIOs. More specifically, the federal CIO's plan identified four tenets to guide Federal Information Security Modernization Act performance management: Movement to Zero Trust Architecture, Ground Truth Testing, Observable Security Outcomes, and Automation.**

**a. What are the federal CIO's responsibilities specific to cybersecurity implementation?**

---

<sup>10</sup> <https://www.cisa.gov/directives>

- b. How is OMB tracking implementation of these three directives?**
- c. Is this implementation progress publicly available? If not, why not?**
- d. What more can Congress do to advance these initiatives?**

**Answer:** OMB has statutory responsibility for overseeing agency information security policies and practices. That responsibility includes authority to develop and oversee the implementation of information security policies and standards and to supervise agency efforts to ensure that IT activities incorporate adequate, risk-based, and cost-effective security. 44 U.S.C. § 3553(a). The Federal CIO spearheads OMB’s fulfillment of those responsibilities. *See* 44 U.S.C. § 3602 (discussing the responsibilities of the Administrator of OMB’s Office of Electronic Government—another name for the Federal CIO); *see also* GAO-22-104603, *Chief Information Officers: Private Sector Practices Can Inform Government Roles* 30-32 (2022).

The Information Technology Operating Plan<sup>11</sup> was submitted to Congress pursuant to a request in the Joint Explanatory Statement accompanying the Consolidated Appropriations Act, 2022. The Joint Explanatory Statement asked OMB to provide a plan to “maximize the impact” of funds provided for the Technology Modernization Fund, the Information Technology Oversight and Reform account, the Federal Citizen Services Fund, and the United States Digital Service. The Information Technology Operating Plan lays out a unified approach for the IT organizations at the center of the Federal Government to fund impactful IT investments, including those for cybersecurity.

EO 14028 directs multiple agencies, including OMB, to take steps to enhance cybersecurity through a variety of initiatives. The guidance OMB has issued pursuant to the Executive Order is made publicly available at <https://www.whitehouse.gov/omb/information-for-agencies/memoranda/>. Further, OMB is using the annual FISMA guidance and CIO metrics to track agency implementation of EO 14028. OMB plans to publish targeted information on agency cybersecurity performance, which will include tracking the progress agencies are making towards implementing certain parts of the EO, in December 2022.

Separately, OMB has continued to engage agency IT leadership on their progress in achieving goals set forth by OMB. Through Communities of Practice, as well as in one-on-one “deep dives,” staff from the Office of the Federal Chief Information Officer (OFCIO) work to assess agency progress and provide support, as necessary.

- 4. In 2018, Congress enacted the 21st Century Integrated Digital Experience Act (IDEA) Act, which directed federal agencies to transform the way they interact with and serve the public online through seemingly simple tasks like making federal websites more user-friendly. Unfortunately, many agencies have struggled to implement some of the reforms. Many people,**

---

<sup>11</sup> [https://www.whitehouse.gov/wp-content/uploads/2022/06/Federal-IT-Operating-Plan\\_June-2022.pdf](https://www.whitehouse.gov/wp-content/uploads/2022/06/Federal-IT-Operating-Plan_June-2022.pdf)

**especially those with disabilities, need to access federal services they depend on.**

**a. How are you ensuring that agencies are effectively implementing the IDEA Act?**

**b. Is this information publicly available? If not, why not?**

**Answer:** As part of the 21st Century Integrated Digital Experience Act of 2018 (Pub. L. No. 115-336), agencies are required to report annual implementation progress to OMB in a publicly available report every year thereafter for 4 years of enactment. OMB has encouraged agencies to use this report to highlight successes, priorities, and challenges with regards to website modernization, form and service digitization, and customer experience. OMB reviews these reports along with additional information when reviewing and discussing agency IT performance.

Currently, OMB is exploring additional ways to ensure agencies are effectively implementing the 21st Century Integrated Digital Experience Act, which include but are not limited to improving data collection and public reporting of agency's website progress beyond these annual implementation reports and exploring the need for additional guidance to further assist agency implementation efforts.

OMB has asked agencies to make their annual 21st Century Integrated Digital Experience Act implementation reports publicly available on their website (e.g., [www.agency.gov/digitalstrategy/](http://www.agency.gov/digitalstrategy/)). In addition, OMB is also working with the General Services Administration (GSA) on better ways to collect and publicly display more detailed information about agency websites so that the public and Congress can assess the compliance of those sites with Federal standards on security, design, accessibility, and compatibility with mobile devices.

**5. The federal CIO's Information Technology Operating Plan notes that "[a]gencies frequently struggle to build and maintain high quality websites that meet the needs of all users while conforming to industry best practices, relevant policies, and laws."<sup>12</sup>**

**a. What specific challenges do agencies face in this arena? For example, are these struggles related to long-term maintenance, use of open-source software, etc.?**

**Answer:** Agencies face numerous challenges to build and maintain high quality websites that meet the needs of all users while conforming to industry best practices, relevant policies, and law. Challenges vary by agencies and include: insufficient training on the use of a human-centered design approach to deliver for customers, budgetary constraints, procurement friction, digital workforce and organizational challenges, the need for more support in the form of senior leadership teams being aligned and engaged in the work, and the need for additional Government-wide resources and common products, platforms, and services.

---

<sup>12</sup> The White House, Information Technology Operating Plan (June 2022) (online at [www.cio.gov/assets/files/Federal-IT-Operating-Plan-June-2022.pdf](http://www.cio.gov/assets/files/Federal-IT-Operating-Plan-June-2022.pdf))

- 6. Last year, the Biden Administration published Executive Order 14058, which focuses on improving customer experience and service delivery between the federal government and the public. It states that positive customer experience is key to rebuilding the public’s trust in the government, which should deliver the level of service that the public expects and deserves.**
- a. Please provide an update on your progress implementing EO 14058.**
  - b. What role can the FITARA Scorecard play in holding agencies’ feet to the fire to adopt customer-centric practices?**

**Answer:** Executive Order (EO) 14058 on Transforming Federal Customer Experience and Service Delivery to Rebuild Trust in Government lays out 36 customer experience commitments across 17 Federal agencies that help improve people’s lives and the delivery of Government services. The EO also establishes a Government-wide approach and priority around improving service delivery and customer experience.

During the first 9 months of implementing the EO, we have discovered key pain points and opportunities in the designated life experiences,<sup>13</sup> and we are seeing progress on agencies’ specific CX EO commitments. For example, veterans can easily view and cancel appointments, receive push notifications when they receive a message from their healthcare provider, and quickly check disability claims and appeal statuses via VA’s new mobile app; SSA is expanding an online service for recently married residents who want to update their Social Security card to reflect their new name without traveling to a Social Security office; and TSA has started to allow passengers to use an authenticated mobile ID during TSA’s airport screening, decreasing processing time and enabling a “touchless” experience.

As we approach the end of this year, OMB will encourage agencies to demonstrate the results of their individual commitments and life experience projects to show the public the progress they are making to improve Federal customer experience. We look forward to continuing to sharing progress updates with Congress and the public on [performance.gov/cx](https://www.performance.gov/cx).

Since technology powers almost all aspects of the customer experience, the FITARA Scorecard can be a useful tool to ensure that the Federal Government continues to deliver simple, seamless, and secure services to the public. Agency CIOs lead the way in improving Federal customer experience by building more modern IT systems; building security, trust, and safety into every interaction; designing tools and services with the public in mind; and using data to drive agency service decisions. Continuing to hold agencies accountable in these critical areas will help deliver excellent, equitable, and secure Federal services and customer experience to the American people.

- 7. The Government Accountability Office found that a qualified, well-trained cybersecurity workforce is vital to operating and protecting federal IT**

---

<sup>13</sup> <https://www.performance.gov/cx/blog/redesigning-how-gov-delivers-services/>

systems.<sup>14</sup>

- a. **Is the federal CIO coordinating with the Office of Personnel Management and the National Cyber Director on their new IT workforce plan?**
- b. **If so, what is the federal CIO's role in this arena?**
- c. **What additional laws, policies, or resources do you need to build a workforce ready to ensure government can address the technology and security challenges it faces and will face in the future?**

**Answer:** OMB is currently working with additional Federal partners, including the Office of Personnel Management (OPM), the Office of the National Cyber Director (ONCD), the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) Councils, and the Chief Human Capital Officer (CHCO) Council to ensure the Federal Government can better compete for and develop cyber talent amidst a tight national labor market, with a strategic focus on helping agencies be able to bring on and keep new talent, versus simply having agencies acquire each other's existing workers. OMB, including the Office of the Federal CIO, is part of a team, led by National Cyber Director Chris Inglis, working to develop a National Cyber Workforce and Education Strategy.<sup>15</sup> The National Cyber Workforce and Education Strategy aims to address challenges and opportunities in critical areas, improve collaboration across Government-wide efforts, help align resources to aspirations, and implement Biden-Harris Administration priorities on education and workforce development.

The Office of the Federal CIO is currently working with partners in OMB (including the Office of Performance and Personnel Management, the U.S. Digital Service, and Resource Management Offices), OPM, and the ONCD to look at creative ways to address these needs. OPM has provided certain Government-wide cyber flexibilities and is evaluating potential legislative proposals designed to provide agencies with enhanced streamlined pay authorities and flexibilities, including for occupations considered critical.

8. **Much of the federal CIO's role is to coordinate federal IT-related activities governmentwide. The federal CIO must facilitate conversations across agency silos and find ways to improve government performance and promote innovation that will improve federal operations beyond the boundaries of a single agency. Moreover, the missions of federal agencies vary across government—from rebuilding our nation's infrastructure to serving our veterans.**

---

<sup>14</sup> Government Accountability Office, High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas (GAO-21-119SP) (Mar. 2021) (online at [www.gao.gov/highrisk/ensuring-cybersecurity-nation](http://www.gao.gov/highrisk/ensuring-cybersecurity-nation)).

<sup>15</sup> <https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/21/fact-sheet-national-cyber-workforce-and-education-summit/>

- a. **How can the federal CIO track and measure success across such varied agencies and their missions?**
- b. **Though government and industry often have different missions, what best practices can you or other agency CIOs use from the private sector to better manage IT, inform decisions, and analyze costs?**

**Answer:** We must recognize the diversity of agencies in their IT maturity to understand how we can move forward as a Federal Government. Enterprise collaboration is essential. By sharing effective and promising practices and lessons learned from those who experience success – including industry partners – and evaluating the unique challenges our agencies face, we can drive and sustain progress. Additionally, leveraging data as a strategic asset can enable an enterprise view, provide better insights to agencies’ modernization journeys, and optimize strategic investment decisions.

**9. The President’s Management Agenda focuses on (1) increasing the number of agencies that facilitate the use of IT and other cloud-based collaboration tools, which support interoperability and (2) cross-agency work to adopt multi-agency document collaboration and sharing platforms.<sup>16</sup>**

- a. **How are you measuring agencies’ progress to achieve both goals?**
- b. **How many agencies are using a single cloud strategy? How many are using a multi-cloud strategy?**
- c. **In addition to data on the cloud services and providers agencies use, what other data is the Office of Management and Budget (OMB) collecting on agencies’ cloud assets? For example, what metrics are you using to (i) track the migration process; (ii) assess Federal cloud adoption practices; and (iii) assess customer experience?**
- d. **How is OMB working with the General Services Administration (GSA) to improve and optimize the Federal Risk and Authorization Management Program?**

**Answer:** Data relevant to progress in achieving these two milestones, which are part of the President’s Management Agenda and Cross Agency Priority (CAP) goal to “Reimagine and build a roadmap to the future of Federal work informed by lessons from the pandemic and nationwide workforce and workplace trends,” is tracked and published on performance.gov, which is updated quarterly. For example, twenty of the CFO Act agencies have signed agreements to safelist 10 FedRAMP approved collaboration tools. Safelisting the 10 FedRAMP-authorized software tools means the agencies enable their agency users to have web access to the tools, and enables other agencies to have access to these web tools.

---

<sup>16</sup> The White House, The Biden-Harris Management Agenda Vision: Toward an Equitable, Effective, and Accountable Government that Delivers Results for All (Nov. 2021) (online at [www.assets.performance.gov/PMA/Biden-Harris\\_Management\\_Agenda\\_Vision\\_11-18.pdf](http://www.assets.performance.gov/PMA/Biden-Harris_Management_Agenda_Vision_11-18.pdf)).



OMB is not tracking whether agencies are using a single or multi-cloud strategy, because the ability to adopt cloud-based collaboration tools and engage in multi-agency collaboration is not contingent on use of one strategy or the other. Data regarding agency cloud migration processes, adoption practices, and customer experience are also not needed to assess whether agencies are able collaborate with each other using cloud-based technologies.

As part of efforts to make improvements to FedRAMP, OMB has spent this past year interviewing interagency stakeholders and evaluating what improvements could be made with the goal of garnering trust and reuse of authorizations across agencies, creating a flourishing marketplace of cloud technologies given emergence of new software-as-a-service (SaaS) offerings, and encouraging automation to make FedRAMP processes work better for cloud service providers and agencies. OMB has also spent a significant amount of time working with Congressional sponsors of legislation authorizing and codifying the FedRAMP program to ensure that the legislation provides FedRAMP with the authority and flexibilities to meet the needs of its customers.

**10. The federal CIO worked with the federal Chief Information Security Officer to revise the metrics requested from agencies to ensure they are employing proper cybersecurity practices. How have you ensured that mobile technologies like iPads and mobile phones are included in these metrics? More generally, what are you doing to ensure the cybersecurity of mobile technologies, which are increasing in use?**

**Answer:** Mobile device security is covered under Executive Order (EO) 14028 and M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response. M-22-01 directs agencies to coordinate with the Cybersecurity and Infrastructure Security Agency (CISA) to accelerate their adoption of robust endpoint detection and response (EDR) solutions, an essential component for zero trust architecture that combines real-time continuous monitoring and collection of endpoint data (for example, networked computing devices such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities. A range of diverse endpoints and what were traditionally considered mobile devices (i.e., tablets and smartphones) are converging. This can be seen in devices like Chromebooks, “Internet of Things” devices, and even fleets of vehicles. Not only has this made interpretations of what is and is not a mobile device harder to discern, but there is no longer a reason for OMB to require agencies to distinguish between them.

That does not mean we are requiring any less of mobile technologies—in fact, it is quite the opposite. As our tablets, smartphones, and other mobile devices gain computing power, specialization, and sophistication, they increasingly require the same security outcomes as other endpoints.

OMB and our partners at CISA are dedicated to capturing agency reporting on all devices using accurate machine-readable information to determine agency performance. As laid out in EO 14028 and M-22-09, agencies are required to participate in

Continuous Diagnostics and Mitigation (CDM), which includes an Enterprise Mobility Management feature. This requirement includes creating ongoing, reliable, and complete asset inventories. CISA’s Binding Operational Directive 23-01, Improving Asset Visibility and Vulnerability Detection on Federal Networks, will also drive further vulnerability enumeration on these devices. OMB Memorandum M-22-01 requires agencies to deploy EDR solutions that provide real-time continuous monitoring and collection of endpoint data—explicitly mentioning mobile phones—with rules-based automated response and analysis capabilities. Mobile device security is one of many areas that we discuss in our conversations with agencies on issues ranging from identity, credential, and access management to their broader Zero Trust implementation plans.

OMB is dedicated to ensuring every Federal endpoint adheres to our Zero Trust Strategy; we continue to build visibility and monitor this approach in the FISMA metrics to ensure high fidelity of understanding regarding the landscape of Federal devices—both mobile and traditional.

**11. On July 15, OMB officials provided the Subcommittee with a briefing on their ideas to evolve the FITARA Scorecard.**

- a. One proposed change to the PortfolioStat category focused on pivoting away from measuring IT spending savings and towards ensuring optimal IT security and IT mission effectiveness. What is your office’s next step to assist the Subcommittee to evolve the PortfolioStat category?**
- b. Another proposed change included a new “Website Metrics” category. Please update the Subcommittee on your progress for this new category, the data you are collecting, and the work you have already completed with GSA.**

**Answer:** Under FITARA and the FITARA Enhancement Act,<sup>17</sup> OMB and agencies are required to report data about cost savings associated with their portfolio of IT investments. Additionally, FITARA requires OMB to “develop standardized cost savings and cost avoidance metrics” for agencies to review and report their portfolio of IT investments as directed by the statute (40 U.S.C. § 11319(d)(2)). FITARA also requires OMB to submit a quarterly report on cost savings and reductions in information technology investments, which is published on ITDashboard.gov. However, as many agency CIOs note, cost savings can be difficult to find since modern and secure IT solutions often cost as much as, if not more than, an antiquated approach. Without a change in statute, evaluating agencies’ effectiveness in managing their information technology investments will continue to focus on cost savings and cost avoidance, rather than the most modern and secure solutions.

I also look forward to OMB publicly releasing new website metric data with GSA in early 2023. GSA is currently developing a tool that would regularly scan Federal

---

<sup>17</sup> 40 U.S.C. § 11319

websites and automatically analyze them for key metrics related to security (HTTPS), design (USWDS), analytics, accessibility, and compatibility with mobile devices.

**Questions for Ms. Clare Martorana**  
Federal Chief Information Officer

**Questions from Rep. Shontel Brown**

September 16, 2022, Hearing: “Project Federal Information Technology: Make IT Work”

---

- 1. As the executive branch agencies work to modernize their websites and digitalize services, what efforts are you all making to ensure website accessibility, keeping those who struggle with technology most in mind?**

**Answer:** Web accessibility is critical to digital service delivery, and it is essential to maximize the ability of all members of the public to navigate Government programs and services. OMB continues to direct agencies to prioritize IT accessibility efforts, especially when an agency is modernizing websites or digitizing forms and services that impact service delivery.

Since 2013, Federal agencies have been required to report to OMB twice per year on their IT accessibility and Section 508 program maturity and effectiveness. Those reports include information on the accessibility of agency websites. OMB analyzes these reports as preparation for its IT performance management conversations with agencies and to better inform Government-wide accessibility efforts. OMB is continuing to track agencies’ progress on accessibility to make sure they are prioritizing accessibility, remediating existing accessibility issues, and making progress toward the delivery of more accessible IT.

Finally, under Executive Order 14035, Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce, as well as under the Government-Wide Strategic Plan to Advance Diversity, Equity, Inclusion, and Accessibility in the Federal Workforce, OMB is working with GSA, U.S. Access Board, Department of Justice, and the CIO Council to review existing accessibility guidance, resources on effective and promising practices, and reporting efforts in order to better help agencies build and sustain an accessible Federal technology environment.

- 2. What progress is being made to develop a diverse cybersecurity workforce as we strive to protect America’s digital infrastructure? Additionally, what efforts are being made to engage with public universities and community colleges, not just elite private institutions.**

**Answer:** The Administration believes our Government is at its best when the Federal workforce draws from the full diversity of our nation and everyone has a chance to fulfill a call to public service. The President’s Management Agenda (PMA) Priority 1, Strengthening and Empowering the Federal Workforce, illustrates our commitment to attracting new talent, building the talent pipeline, and investing in retaining and revitalizing our current workforce.

To grow our talent pool, we have to look beyond the traditional pool of “cybersecurity

or IT talent.” We need to recruit diverse talent that is underrepresented in the Federal workforce today, create more opportunities for graduates and junior professionals, and invest in K-12 programs that can support students who are interested in pursuing work in the technology field. OMB is currently working with Federal partners, including OPM, ONCD, and the CIO, CISO, and CHCO Councils, to ensure the Federal Government can better compete for and develop cyber talent amidst a tight national labor market. Additionally, the Administration is working to develop a National Cyber Workforce and Education Strategy, which will address the challenges and opportunities in critical areas, improve collaboration across Government-wide efforts, help align resources to aspirations, and implement Administration priorities on education and workforce development.

**Questions for Ms. Clare Martorana**  
Federal Chief Information Officer

**Questions from Ranking Member Jody Hice**  
Subcommittee on Government Operations

September 16, 2022, Hearing: “Project Federal Information Technology: Make IT Work”

---

1. **During the hearing, in response to my first question about the Administration’s failure to issue Cross-Agency Priority (CAP) goals on time, you replied that OMB is technically in compliance with GPRA because the Administration has until the end of the full first fiscal year to designate CAP goals which you say it did so on August 9th of this year.**

**Section 1120 of title 31, United States Code, requires CAP goals to be made publicly available “concurrently with the submission of the budget of the United States Government.” The statutory provision continues by specifying that the budget submission in question is the one “made in the first full fiscal year following any year in which the term of the President commences.”**

**Additionally, OMB’s circular No. A-11,<sup>18</sup> the fiscal year 2024 budget guidance, states that the “GPRA Modernization Act of 2010 requires CAP Goals to be made publicly available concurrently with the submission of the President’s Budget in the first full fiscal year following any year in which the term of the President commences.” (Emphasis added.)**

- a. **Is it the Administration’s position that section 1120 and OMB’s Circular No. A-11 require CAP goals be made available before the end of the first fiscal year rather than concurrent with a budget submission?**
- b. **Please elaborate on the legal reasoning in support of this interpretation.**

**Answer:** To clarify my earlier testimony, the position of the Administration is that “publicly available concurrently with the submission of the budget of the United States Government” means publicly available at the same time the President’s Budget is submitted to Congress, typically in February per statute. Importantly, however, designation of a CAP Goal is used to leverage cross-agency coordination in order to drive execution on an Administration’s management priorities, which are articulated in each Administration’s President’s Management Agenda (PMA). The Biden-Harris PMA Vision was released in November 2021. The CAP Goals on performance.gov identified in August 2022 reflect the greater specificity needed to implement and deliver on the broader outcomes and priorities in the Biden-Harris PMA. We look forward to providing regular progress updates on Performance.gov so that both

---

<sup>18</sup> Circular No. A-11, Preparation, Submission, and Execution of the Budget (August 2022).

Congress and the public can follow the Government's actions and accomplishments.

2. **Since the Committee's July 2022 hearing on FITARA, OMB has labelled several strategies in the President's Management Agenda as Cross-Agency Priority (CAP) goals on the website Performance.gov. Although the Government Performance and Results Act Modernization Act (GPRAMA) of 2010 requires that OMB develop CAP goals for IT management, there do not appear to be any CAP goals related to IT management or cybersecurity. Is this the final set of CAP goals, or will goals be added relative to IT management and cybersecurity? And if so, when?**

**Answer:** There are no plans at this time to add additional CAP Goals. Cross-agency efforts in IT management are currently being advanced as foundational to the success of all of the areas of the Biden-Harris PMA. The Biden-Harris PMA Vision called out IT modernization and cybersecurity as key enabling capabilities for effective and efficient mission delivery across the PMA.

In addition, some of the Administration's CAP Goals focus specifically on agency outcomes driven by IT management and cybersecurity, consistent with GPRAMA. These goals include:

- One of our goals under PMA Priority Area 1, Strengthening and Empowering the Federal Workforce, is to better equip the Federal Government to achieve agency missions and serve the American people by investing in its people, technology, and space. To get there, agencies will facilitate use of IT and other cloud-based collaboration tools that support interoperability, in addition to working together to adopt multi-agency document collaboration and sharing platforms.
- For PMA Priority Area 2, Delivering Excellent, Equitable, and Secure Federal Services and Customer Experience, IT management and cybersecurity are central to all designated CAP Goals. For this reason, I am one of several executive-level leaders of the Administration's customer service initiative within OMB. These CAP goals include:
  - "Improve the service design, digital products, and customer-experience management of Federal High-Impact Service Providers by reducing customer burden, addressing inequities, and streamlining processes"—this work requires in many cases IT modernization activities within agencies.
  - "Design, build, and manage Government service delivery for key life experiences that cut across Federal agencies"—also here, IT modernization activities within agencies are key.

Actions to advance CAP goals are currently tracked as "Initial Milestones" on performance.gov, and success metrics are posted publicly there as well.

Additionally, while CAP Goals are updated or revised every 4 years, per statute, the Director of OMB may make adjustments to the CAP Goals as needed at any time to reflect significant changes in the environment in which the Federal Government is operating. Such 'environmental scanning' is a regular part of OMB's internal

management and review process for delivering on the PMA vision.

**3. In place of CAP goals related to IT management and cybersecurity, what other government-wide goals, strategies and performance measures are you using to assess progress in IT management and cybersecurity government-wide?**

**Answer:** The PMA is one of many avenues to track IT management and cybersecurity. OMB regularly releases policy, guidance, goals, and strategies through formal circulars and memoranda to guide agencies in adopting best practices in IT management and cybersecurity, and OMB conducts formal data calls and informal exchanges with agencies as part of its oversight of various initiatives. For example, OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, established critical milestones that agencies should meet to reinforce Federal agency defenses against increasingly sophisticated adversaries. The Office of the Federal CIO tracks these milestones informally through regular engagement with agencies and through the collection of formal quarterly metrics.

As described in my testimony, OMB plans to publish information about agency cybersecurity performance in December 2022. This will provide Congress and the public with a picture of how agencies are performing on key Federal cybersecurity indicators. Because cybersecurity datasets can be complex, our goal when releasing cybersecurity data is to allow Congress, stakeholders, and the public to view and track progress the Federal agencies are making to secure their systems as well as the areas where improvements and investments may need to be made.

We know that cybersecurity is a field of rapid evolution, and that the Government's defensive practices must keep pace with the capabilities of our adversaries, which is why we regularly assess and refine our metrics to ensure we are accurately measuring agency progress. For example, we recently re-baselined our current FISMA CIO metrics to collect background and overarching information about a new and relevant set of cybersecurity practices. In addition to the FISMA CIO metrics, the Federal cybersecurity community relies on regular audits of agency cybersecurity through agency Inspectors General, as required by FISMA. These complementary methodologies enable the assessment of agency progress and allow us to track longitudinal improvements over time.

**4. During the hearing, following my first round of questions, Mr. Connolly and you engaged in a discussion to clarify a question about the meaning of agencies' partial repayment of Technology Modernization Fund (TMF) awards. Mr. Connolly observed that, "the fact there've been partial repayments is not a substitute for the ultimate, full repayment, but it's providing more flexibility." To which you replied, "Correct."**

**To further clarify, are you saying that agencies that "submit for Board consideration projects requiring repayment terms that represent partial**



**repayment (75%, 50%, or 25% repayment), or minimal repayment”<sup>19</sup> would still be required to repay the full 100% amount of the award?**

**Answer:** No, that is not what I intended to convey. To clarify, I interpreted Chairman Connolly’s comment to mean that – collectively – partial repayment is not the same as full repayment. The TMF Board has always required repayment, and our intent is to require *full* repayment wherever possible. When evaluating project proposals, the TMF Board looks for outsized returns and repayment – starting at *100 percent repayment* as a baseline. However, we also look at the impact and circumstances of the project to adjust repayment accordingly. There are many benefits to offering partial repayment – including providing more flexibility and promoting a diverse set of project proposals. Partial repayment is not the baseline repayment rate. We continue to require full repayment for investments when appropriate. The Board is operating in line with the legal requirement to ensure the solvency of the fund. GAO concurred with this approach in its decision published on July 14, 2022.<sup>20</sup>

**5. In testimony provided to the committee for a TMF hearing in May,<sup>21</sup> the GAO witness explained that:**

- i. OMB and GSA “have not yet fully implemented our recommendation to develop and implement a plan to fully recover operating expenses with fee collection.”<sup>22</sup>**
- ii. The GAO witness further said that “it is not clear when the [TMF Program Management] office will fully recover future operating expenses incurred in fiscal year 2022 and beyond.”<sup>23</sup>**
- iii. The GAO testimony also notes that the majority of TMF projects awarded through August 2021 have not realized cost savings.<sup>24</sup>**

**Yet, in May 2021, OMB updated its funding guidelines to agencies for TMF reimbursement by allowing agencies to apply for “partial or minimal reimbursement of their awards.”<sup>25</sup>**

**Given points i, ii, iii, and OMB’s guidance in 2021, please explain how the TMF Board expects to meet the requirement of the MGT Act to “ensure the solvency of the Fund, including operating expenses.”<sup>11</sup>**

**Answer:** On July 14, 2022, GAO issued GAO B-333396, which concluded “that the Office of Management and Budget (OMB) and the General Services Administration

<sup>19</sup> TMF Website, Funding Guidelines for Agencies Receiving Disbursements from the Technology Modernization Fund.

<sup>20</sup> <https://www.gao.gov/products/b-333396>

<sup>21</sup> May 25, 2022, Oversight and Reform Subcommittee on Government Operations Hearing, Technology Modernization Fund: Rewriting Our IT Legacy.

<sup>22</sup> GAO Testimony, May 25, 2022, Oversight and Reform Subcommittee on Government Operations Hearing, Technology Modernization Fund: Rewriting Our IT Legacy.

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> *Id.*

(GSA) may require less than full reimbursement, provided the reimbursement rates are sufficient to satisfy the statute's solvency requirement, and are not inconsistent with other statutory objectives."<sup>26</sup> The TMF account balance is positive, and the fund continues to be financially solvent. As part of the annual budget formulation and TMF planning process, OMB and GSA have had, and continue to have, a process in place to ensure that resources to support the expenses of the TMF Program Management Office are sufficient to fulfill the requirements outlined in the Modernizing Government Technology Act and will remain available through the fund's existence.

GSA controls to ensure TMF solvency include the following:

- 1) The TMF maintains a positive cash balance with Treasury.
- 2) The TMF maintains positive budgetary resources at all times (as reported on the SF-133).
- 3) The TMF maintains budgetary resources sufficient to pay for existing and anticipated obligations through the fund's existence (5 years after the sunset provision).
- 4) PMO expenses are set aside (not available for transfer) for the current fiscal year and the next fiscal year to ensure adequate funding.
- 5) Collections are not made available for transfer until the year following the year when the collection is recorded to ensure that plans are not made for resources that are not yet realized.

**6. Understanding that the cybersecurity posture of federal agencies is a priority for congressional oversight, how has the FITARA Scorecard made a meaningful impact on agency cyber resiliency?**

- a. What improvements have we seen over the years with the FITARA Scorecard?**
- b. How can the Subcommittee improve the scorecard metrics in this critical area to improve congressional oversight of government-wide cyber resiliency of our federal information systems without letting our adversaries know our weaknesses?**

**Answer:** The FITARA Scorecard was first introduced nearly 7 years ago to track agency implementation of the FITARA statute. Since that time, we have seen CIOs have greater oversight of their agency IT investments and agencies themselves have made vast improvements managing their IT.

The FISMA metric of the FITARA Scorecard was added in 2018. While it could be meaningful to track cybersecurity in the FITARA Scorecard, we should make sure that the Scorecard tracks impactful measures that maximize our ability to buy down risk. For example, the data that was previously published in the prior Administration through performance.gov, and used in the FITARA Scorecard, reflected internal agency assessments based on completion of compliance activities. Many of those assessments did not accurately reflect whether an agency had implemented good

---

<sup>26</sup> <https://www.gao.gov/products/b-333396>

cybersecurity toolsets and practices. Releasing compliance-oriented data does not increase agencies' accountability or facilitate public oversight. In fact, continuing to release such data provides a false sense of confidence to the public and to Federal entities that are not advancing their cyber defenses, and ultimately marginalizes the real work being done by Federal agencies to modernize their cybersecurity approach.

Additionally, the Scorecard's use of IG assessment ratings to grade agencies does not accurately represent the current posture of a particular agency's information security practices. The current model used by OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) to evaluate agency information security programs for effectiveness is based on the Capability Maturity Model Integration (CMMI) model published by the Software Engineering Institute (SEI). This is an industry standard used across the cybersecurity sector. FISMA requires that agency IGs gauge the effectiveness of information security programs and practices. Under OMB's guidance for IG assessments, an agency's information security program is considered effective if it achieves a rating equal to *Level 4 – Managed and Measurable*. That approach is consistent with the way in which private sector organizations evaluate the effectiveness of their cyber programs and practices. However, agencies that achieve a Level 4 rating are assigned only a B on the FITARA Scorecard.

When looking at how the FITARA scorecard is currently calculated, our understanding is that a straight division calculation is being used to assign an uncomplicated grade to agency performance. That simple calculation method does not provide an accurate view of the maturity levels assessed by IGs' FISMA evaluations, however.

Cybersecurity is a field of rapid evolution, and the Government's defensive practices must keep pace with the capabilities of our adversaries. OMB is working with CISA and ONCD to assess what cybersecurity data collected from agencies through the FISMA CIO metrics would be appropriate to share publicly. OMB is working towards the publication of targeted cybersecurity performance data in December 2022. The public data will allow Congress and the public to track agency progress in implementing E.O. 14028 and OMB policies on multifactor authentication, encryption, and other important cyber actions. Our goal in releasing cybersecurity data is to focus agencies and the public on an accurate picture of the security of Federal systems and the areas where investments need to be made. We must also balance transparency with security concerns, and ensure that these potentially sensitive datasets are shared in a way that does not focus adversary attention on potential gaps to exploit. Based on our learnings in FY 2022, we intend to further adapt the FISMA CIO metrics to ensure we can continue to evaluate agency progress in protecting their systems from new and evolving cyber threats, while providing the public with information about agency progress. We look forward to working with the Subcommittee to improve the Scorecard's FISMA metric and facilitate Congressional oversight of Government-wide cyber resilience.

- 7. The FITARA Scorecard is supposed to grade agencies on their implementation of provisions of the FITARA law, but recent Scorecards have included categories that were not in the law. Has the addition over the years of non-FITARA-related categories to the Scorecards made the**

## **Scorecards more effective in serving their intended purpose? Why?**

**Answer:** The FITARA Scorecard reflects the priorities of the Subcommittee on Government Operations regarding the specific areas of information technology management the Subcommittee would like agencies to focus on. Due to the oversight nature of the Scorecard, agencies will seek to make improvements in any category added by the Subcommittee whether or not the category is based in statute. Looking forward, when the Subcommittee aims to assess agencies in an area outside of the FITARA statute, the CIO community – including the Office of the Federal CIO and the CIO Council – is available to provide valuable input to ensure the methodology behind the grading for that category is accurate and measures meaningful output.

### **8. The GSA FedRAMP program is a crucial part of ensuring the security of federal agency cloud computing systems. What kinds of metrics could be used to track agencies' progress in utilizing the FedRAMP program? Are there ways to incentivize agencies to take advantage of the FedRAMP program?**

**Answer:** The GSA FedRAMP program is a valuable security program in the Federal Government. My office is currently working with GSA to ensure that we expand the program into a flourishing marketplace of diverse cloud products and services and that agencies look to FedRAMP first as an authoritative and efficient path to onboard modern and secure cloud offerings. The FedRAMP Marketplace (<https://marketplace.fedramp.gov/#!/products>) already tracks agency reuse of FedRAMP authorizations, and could be explored as a potential metric. The efficiencies and cost savings associated with the principle of “do once, use many times,” combined with an expanded and more diverse marketplace of approved cloud products and services, are a significant incentive for agencies to leverage FedRAMP. OMB will work with GSA and other agencies on methods to encourage more agencies to take advantage of the offerings available to them.

### **9. The IT Dashboard is a website designed for “public consumption”, yet the accuracy and relevance of the information is unclear.<sup>27</sup> For example, agency CIOs are expected to use their best judgment to rate investments “using a set of pre-established criteria.”<sup>28</sup> While this includes “risk management” as an evaluating factor, the IT Dashboard does not appear to provide a consistent definition of risk management, and it is unclear if all agencies use the same definition for risk management.**

#### **a. Do all agencies use the same definition of “risk management” when providing data to the IT Dashboard? If so, what is that definition, and where is that definition provided?**

**Answer:** The IT Dashboard’s “FAQ” section includes general information on how data is reported to the IT Dashboard, including how CIOs evaluate specific factors such as risk management. More specific information can be found in Circular A-11 and other

---

<sup>27</sup> ITDashboard.gov.

<sup>28</sup> ITDashboard.gov, FAQ – CIO Evaluations.

OMB guidance.

“Risk management” is generally defined in Circular A-11 and Circular A-123 as a “systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk,” which aligns with International Organization of Standardization (ISO) standards.

Agency CIOs are ultimately responsible for evaluating IT investments and assessing each investment’s level of risk. Agency CIOs do have some discretion when making this assessment. However, their evaluation must be informed by OMB’s guidance and best practices, including definitions, and should assess elements such as risk management, requirements management, contractor oversight, historical performance, human capital, and other factors the agency CIO deems important to forecasting future success. OMB has also provided criteria to aid in assessing risk management, instructing CIOs to evaluate, for example, whether “risk management strategy exists; risks are well understood by senior leadership; risk log is current and complete; risks are clearly prioritized; and mitigation plans are in place to address risks.”

**10. Does OMB have a definition of “legacy system?”**

**Answer:** Section 1076 of the National Defense Authorization Act for Fiscal Year 2018<sup>29</sup> defines a “legacy information technology system” as “an outdated or obsolete system of information technology.” It is important to note that not all “old” systems are legacy, and old does not always mean bad, antiquated, risky, or in need of retirement. A legacy system is outdated or otherwise obsolete – in other words, it is no longer supported, it does not meet the mission needs of an agency, and its security cannot keep pace with our adversaries.

**11. What are the top ten federal IT systems that need to be replaced or otherwise modernized due to their age, inherent risk, and the importance of the associated mission. That is, what are the top ten “legacy systems” that need to be retired?**

**Answer:** I noted earlier that Federal IT systems do not necessarily need to be retired or otherwise modernized due to their age alone – “old” does not necessarily mean bad, antiquated, risky, or in need of retirement. A system’s utility depends on whether it can deliver on its mission. Each Federal Government system must have a secure foundation and be able to deliver for the American people, and this Administration has made IT and cybersecurity a priority. We recognize the diversity of the agency IT landscape, and are actively working with agency CIOs to identify challenges and gaps inhibiting modernization.

However, GAO has assessed systems based on the factors you highlighted above and in April 2021 published GAO-21-524T, “Information Technology: Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems.” That report

---

<sup>29</sup> Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018.

identifies 10 critical Federal IT legacy systems that, in GAO's assessment, are most in need of modernization. I appreciate GAO's review of those systems and, as mentioned previously, will work directly with agency CIOs to drive modernization.

- 12. Does OMB track the state of IT modernization of federal systems? If so, how? If so, why does the IT Dashboard not provide information regarding the number and age of legacy systems at each federal agency? Could such data be made available in an easy to read and understandable format that is consistent across agencies?**

**Answer:** OMB does not specifically track agency IT systems as legacy or not. In an ideal state, IT systems should be in continuous cycle of modernization. It is challenging to label systems in a binary way—not all old systems are legacy, and old does not necessarily mean bad, antiquated, risky, or in need of retirement. The legacy technology I am most concerned with are systems that are no longer supported and whose security cannot keep pace with the methods of our adversaries. For example, even some older systems that maintain a secure and stable backbone have the ability to retrieve information in a modern way, such as through the use of an application programming interface (API) to deliver a new front-end interface.

For these reasons, it would be difficult to publicly track legacy systems consistently for all agencies; however, I am open to considering alternatives to transparently track the IT modernization of Federal systems.

- 13. In your opinion, what is the purpose of the IT Dashboard and what benefit does it provide the public, your office, and federal agency CIOs themselves? In other words, how does it enable oversight of government-wide federal IT, whether externally by the public and Congress, or internally from OMB or agency leadership?**

- a. How could the IT Dashboard be improved to serve as a better tool for all its users?**

**Answer:** The IT Dashboard ([itdashboard.gov](http://itdashboard.gov)) provides a point-in-time snapshot of the cost, schedule, and performance of Federal IT investments. It provides the public with a list of each major IT investment, along with associated data on cost, schedule, and performance, consistent with OMB's obligations under 40 U.S.C. § 11302. It is important to note that while the IT Dashboard enhances agency accountability by showcasing important data points for Congress and the public, agency CIOs must dedicate significant time and resources to report that data. The more time that agency CIOs spend writing reports or collecting data, the less time they have to focus on mission-oriented outcomes.

We are open to feedback on the Dashboard to make it more useful to Congress and the public.

- 14. The Information Technology Operating Plan (ITOP) notes that in 2017, Login.gov was created to offer the public a single account**

**and identity verification process across multiple government programs.**

- a. How has this system protected user privacy and/or addressed any privacy concerns?**
- b. Are government agencies able to access data from other agencies through this shared system?**
- c. Does the Login.gov service compete with other viable commercial solutions? What commercial services does Login.gov utilize?**
- d. How many agencies use Login.gov?**
- e. Have agencies expressed concern over the utility or cost of Login.gov?**

**Answer:** Login.gov, as a shared identity service, allows members of the public to use a single account to gain secure access to over 200 Government services offered by a wide range of participating agencies. Protecting and maintaining the privacy of users' information is a critical function of Login.gov. The Technology Modernization Fund has invested in Login.gov to ensure that it performs that function while making progress toward achieving a sustainable cost model. We defer to GSA any specific questions about Login.gov's implementation, security, and privacy details.

**15. During the hearing, toward the end of my second round of questioning, I posed the following questions which I'm including in this document to ensure a response:**

- a. Can you supply this committee with a copy of your job description?**
- b. How was the Federal CIO position established?**
- c. Do other federal agency CIOs recognize this position, and do they acknowledge the authority of the position over federal IT policy?**

**Answer:** OMB has extensive IT-related authorities and responsibilities under a wide variety of laws, including the E-Government Act of 2002, the Federal Information Security Modernization Act, the Federal Information Technology Acquisition and Reform Act, the Modernizing Government Technology Act, and the SECURE Technology Act. The E-Government Act established within OMB an Office of E-Government to serve as the coordinating point of those many authorities and responsibilities. *See* 44 U.S.C. § 3602. The Act further created the position of an Administrator to oversee the Office of E-Government. *Id.* Although the term "E-Government" has largely fallen out of use, the Administrator and the Office remain, now known more commonly as the Federal CIO and the Office of the Federal CIO.

Generally, as indicated by 44 U.S.C. § 3602, the Federal CIO assists the OMB Director in carrying out all functions required by the E-Government Act and other IT and cybersecurity initiatives. I advise the Director on the resources required to develop and effectively administer IT initiatives, and recommend to the Director changes relating to Governmentwide strategies and priorities for IT and cybersecurity. I assist the OMB Director in setting strategic direction for implementing Federal IT and work with other OMB officials to fulfill OMB's responsibilities with respect to:

- Capital planning and investment control for IT;
- The development of enterprise architectures;
- Information security;
- Privacy;
- Access to, dissemination of, and preservation of Government information;
- Accessibility of IT for persons with disabilities; and
- Other areas of Federal IT.

Collaboration is essential to the role of the Federal CIO, which is why I actively coordinate with the General Services Administration, Office of the National Cyber Director, and other key stakeholders to improve IT practices across the Federal enterprise. Interagency forums, such as the CIO Council, also bring agency IT leadership together to discuss challenges and share solutions.

Federal agency CIOs look to the Federal CIO to provide overall leadership and direction to the executive branch on Federal IT and promote innovative uses of IT. They also seek guidance from the Federal CIO on how to implement statutory requirements and OMB policies related to Federal IT management and cybersecurity. The Federal CIO is also able to leverage the CIO Council to develop recommendations for the Director of OMB on government information resources management policies and requirements. The CIO Council is also used to bring Federal agency CIOs together to share experiences, ideas, best practices, and innovative approaches related to IT management.

**16. How would codifying the Federal CIO position into law improve the Administration's ability to inform Congress about the status and security of the federal government's IT portfolio?**

**Answer:** IT is such a critical part of how we operate the Federal Government and deliver services, and I believe that we should continue to ensure that all C-suite positions, including CIOs, have a seat – and a voice – at their agency's table. With respect to the Federal CIO position, amending the E-Government Act to codify the role of the Federal CIO would more accurately reflect the role and responsibilities of the position and eliminate the confusion between how the position is referred to publicly and what is in statute. But even in the absence of any further codification of the Federal CIO role, the Federal CIO wields substantial influence as the representative of the OMB Director in IT-related matters. *See* 44 U.S.C. § 3602 and response to question 15 above.

**17. As the Director's representative in matters of Federal IT and cybersecurity**



policy, the Federal CIO is responsible for informing Congress about the status and security of the Federal Government's IT portfolio. While the IT Dashboard (itdashboard.gov) provides some insight into the status of Federal IT investments (e.g., cost, schedule, and performance), we recognize that Congress may desire further information on agency IT portfolios. We are committed to working with Congress to evaluate the feasibility of collecting and publishing information at the level of granularity that Congress would like to see. We remain committed to improving transparency with Congress and would welcome a discussion on ways we can support congressional oversight of Federal IT and cybersecurity and improve collaboration to further our shared goal of delivering a better government to the American people. **What is the state of technology based management (TBM) across the federal government? Would widespread adoption of TBM provide a reliable and efficient oversight tool to track whether federal IT projects and systems were delivered on time, on budget and were delivering the intended level of utility and service? How do federal agencies currently measure these criteria?**

**Answer:** OMB introduced the Technology Business Management (TBM) framework as a means to apply a standard terminology to the IT investment analysis and reporting that is made available to the public via the IT Dashboard. OMB continues to mature the use of the TBM framework in its policy and through OMB's Circular A-11 by requiring Federal agencies' continued and expanded implementation of TBM as an authoritative data source. These ongoing efforts will serve to maximize the effectiveness of discussions about the cost and value of IT. I plan to continue to evaluate frameworks such as TBM to ensure that we foster transparency in our IT spending and create actionable data for decision-making, while minimizing the reporting burden on the CIO community.