Questions for Mr. Richard A. Spires
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?**

   Answer: I do not see evidence that agencies are "artificially" inflating their FITARA Scorecard grades, in the sense that agencies use tactics that raise their grades on the Scorecard without making meaningful changes in their IT infrastructure. As I have testified, the Scorecard has been a valuable oversight tool, and it has made a significant positive difference in driving agencies to improve their IT management. But it is also the case that, as evidenced by GAO reports, we are still not near "best practice" at almost all agencies in IT management. That is why I firmly believe that if the Scorecard evolved to cover other critical areas of IT management, it could continue to make a profound positive difference in federal IT. In my recent written testimony, and at the FITARA 10.0 hearing in August 2020, I made specific recommendations on how I believe the Scorecard should evolve, which I summarize below.

   I recommend the following changes be made right away (or phased in as soon as possible):

   - **Add an "IT Modernization Planning" Category –** Meaningful IT modernization starts with good planning. Hence, this category should reflect the maturity and focus on IT modernization within the agency's planning function and enterprise architecture. To measure this category, existing "best practices" for planning and managing IT could be used by either GAO or agency IGs to audit an agency's IT planning capability to arrive at an IT Planning maturity grade.

   - **Combine the "Incremental Delivery" and "Transparency and Risk Management" Categories into a broader "Delivery of IT Programs" Category** – Agency IT modernization occurs through the successful delivery of IT programs. As such, there should be a category that measures the ability of agencies to manage such programs. There are well-understood and documented best practices that can be measured to arrive at a composite grade for this category.

   - **Evolve the "Managing Government Technology" Category to a broader "IT Budget" Category** - This category should add the use of the Technology Business

Management (TBM) taxonomy so agencies better understand the cost elements of their IT budgets. Agencies could be measured on their adoption of TBM, along with the use of benchmarking of their IT services, so that they can compare their performance to other similar-sized agencies and private-sector corporations.

- **Evolve the "Cybersecurity" Category** – This category needs to be revisited - the existing FISMA measures and cybersecurity CAP goals do not accurately measure an agency's cybersecurity posture. The good news is that the recent Executive Order (EO) on cybersecurity, issued in May of 2021, can serve as a blueprint for what federal agencies should be doing to enhance their cybersecurity position. In particular, the EO places special emphasis on agencies implementing a zero-trust architecture, having holistic visibility across one's IT infrastructure, implementing secure guidelines in cloud computing environments, focusing on protecting high-value data and system assets, and dealing with supply chain issues. The EO can serve as the means to more accurately grade an agency's cybersecurity posture.

Longer-term (within the next few years), I would also like to see the following changes:

- **Add an "IT Workforce" Category** – While more challenging to measure, there is hardly a more important category regarding the ability of an agency to properly manage IT. Having the proper IT positions defined and having them filled with individuals that have the requisite knowledge, skills, and abilities (KSAs) is critical to success in any IT organization.

- **Add a "Customer Satisfaction" Category** – IT organizations have customers. A core measure for all agency support organizations should be customer satisfaction. It would be a best practice to administer a standard customer satisfaction survey to all agencies so this category can be added to the FITARA Scorecard.

2. **This Subcommittee has access to the data outlined in the FITARA statute to conduct robust oversight. What additional data reporting requirements would be helpful to codify to continue robust oversight of federal IT management and acquisition?**

   Answer: To date, measures in the Scorecard have been based on available public data reported by the agencies. So, this requirement of what data is available constrains what changes can be made to the Scorecard. As this question infers, it would be helpful if Congress could first define a new FITARA measure, and then there was a collaborative effort of Congress and GAO working with the Administration to determine how to collect the data necessary to support the measure.

In the recommendations I make on evolving the Scorecard measures (see the answer to Question 1 above), there would be new data reporting requirements. Below are the reporting requirements that would be most helpful to provide robust oversight of federal IT management and acquisition.

Data elements for an **"IT Modernization Planning" Category**:

- The agency should have a strategy that recognizes the importance of IT modernization and the retirement of legacy IT systems, with specific IT modernization objectives included in the agency's strategic plan.
- These IT modernization objectives should be driven by agency mission program priorities and be integrated into agency budgets, performance plans, and measures.
- Such IT modernization plans should be captured in and be supported by an agency's enterprise architecture (EA).
- An agency's EA should include the definition and use of functional portfolios, target "to-be" business, technical, and data architectures that drive modernization, and governance that effectively allocates requirements from enterprise, to portfolio, to program or project for implementation.
- Such planning should include an analysis of legacy systems, addressing those systems to be retired and how other existing or new systems will handle such functionality.
- This planning should be captured in an agency EA transition strategy that is aligned with the agency strategic plan and is tracked and updated annually.

Data elements for a **"Delivery of IT Programs" Category**:

- Demonstrated use of appropriate program and project management disciplines.
- Professional development approaches to develop staff to fill critical roles in a program management office (PMO).
- A comprehensive approach to stakeholder engagement and program governance.
- Development and use of a systems development life-cycle (SDLC) that an agency can readily tailor for all types of IT programs.
- Commitment to incremental delivery and demonstrated use of Agile and DevOps techniques in programs, when appropriate.
- Proper and timely program status reporting.

Additional data elements for an **"IT Budget" Category**:

- Degree of the use of the TBM taxonomy for capturing IT costs across an agency.
- Use of TBM to benchmark basic IT commodity services.
- Use of TBM to benchmark complex IT services.

Additional data elements for the **"Cybersecurity" Category**:

- Meeting all the Cybersecurity Executive Order (EO) dates and requirements.
- Meeting DHS Binding Operational Directives.
- Meeting DHS Emergency Directive Requirements.
- Fulfilling all Zero-Trust implementation requirements (including implementation of enterprise multi-factor authentication (MFA) and secure access service edge (SASE) solutions).
- Being responsive to cybersecurity-related audits (meeting deadlines to support IG and GAO work and implementing recommendations per the agreed dates).
- Establishing baseline levels of risk aligned to the OMB's FY 2021-2022 FISMA guidance.[1] (Specifically, the new data elements in Appendix A related to scanning internet-accessible addresses and segments of Federal civilian agency systems for vulnerabilities on an ongoing basis.)

Data elements for a **"Workforce" Category**:

- The agency CIO has a set of competency models for the critical positions in the IT organization.
- The agency has developed career development paths for the more senior IT positions.
- All IT staff in the agency have, as part of their annual review process, formal individual development plans (IDPs).
- The agency has a current IT workforce plan in place, showing where the agency has current workforce talent gaps, along with projections of gaps over a three-year period.
- The agency has established a robust training and development program to support IT workers in meeting their objectives as detailed in their IDP.
- The agency has a comprehensive recruiting approach to address critical IT workforce gaps.

Data element for a **"Customer Satisfaction" Category**:

- An agency administers a standard (used by all agencies) customer satisfaction survey that covers elements of customer experience and service, along with how IT supports an agency in meeting its mission objectives.

Given that some of these measures would require an IG or GAO to audit an agency to determine a grade in a category, it would make sense to move some of the categories to a yearly update, rather than every six months. Likewise, in a customer satisfaction category that includes a survey, such a category should be updated yearly, not every six months.

[1] https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf

3. **What components of the FITARA law should be updated to reflect best federal IT management and acquisition practices?**

Answer: While the FITARA legislation is valuable and an update to the law is warranted, the consistent oversight from Congress has made the real difference, especially the use of the Scorecard to drive agencies to advance IT management in the areas in which the Scorecard measures progress. The predecessor law to FITARA, the Clinger-Cohen Act, never had follow-on Congressional oversight, and as a result, the Clinger-Cohen Act is generally viewed in federal IT as a failure. As such, I urge Congress in the near term to make sure you don't lose focus on evolving the Scorecard to make it even more of a valuable tool in measuring an agency's IT management maturity.

Regarding upgrading FITARA, changes to the law that address the IT management issues I recommend be included in an enhanced Scorecard would be of value. These changes include:

- Codifying the need for agencies to do proper IT modernization planning with specific emphasis on the appropriate analysis of legacy systems and identification and plans for legacy systems that should be retired.
- Outlining how agencies can upgrade their ability to successfully deliver IT programs.
- Requiring the use of TBM for agencies to better understand their IT costs, and to benchmark themselves with other agencies and private-sector corporations.
- Requiring enhanced reporting to support the ability to measure an agency's cybersecurity maturity.
- Adding in the measurement of an agency's ability to recruit, develop, and retain IT staff.
- Including a requirement that a survey is conducted annually rating the customers' satisfaction of agencies' IT departments.
- Broadening the focus on data center consolidation to more general IT Infrastructure optimization by having agencies properly leverage cloud computing and modernizing their networking infrastructures.

4. **What key IT priorities should an updated FITARA Scorecard capture? What is currently missing from the Scorecard?**

Answer: In my recent testimony, as well as my testimony on the 10.0 Scorecard, I described my views on what an updated FITARA Scorecard should capture. Below is a summary of changes that I believe should be made to the Scorecard, which also addresses what is missing from the current Scorecard.

I recommend the following changes be made right away (or phased in as soon as possible):

- **Add an "IT Planning" Category –** Meaningful IT modernization starts with good planning. Hence, this category should reflect the maturity and focus on IT modernization within the agency's planning function and enterprise architecture. To measure this category, existing "best practices" for planning and managing IT could be used by either GAO or agency IGs to audit an agency's IT planning capability to arrive at an IT Planning maturity grade.

- **Combine the "Incremental Delivery" and "Transparency and Risk Management" Categories into a broader "Delivery of IT Programs" Category** – Agency IT modernization occurs through the successful delivery of IT programs. As such, there should be a category that measures the ability of agencies to manage such programs. There are well-understood and documented best practices that can be measured to arrive at a composite grade for this category.

- **Evolve the "Managing Government Technology" Category to a broader "IT Budget" Category** - This category should add the use of the Technology Business Management (TBM) taxonomy so agencies better understand the cost elements of their IT budgets. Agencies could be measured on their adoption of TBM, along with the use of benchmarking of their IT services, so that they can compare their performance to other similar-sized agencies and private-sector corporations.

- **Evolve the "Cybersecurity" Category** – This category needs to be revisited - the existing FISMA measures and cybersecurity CAP goals do not accurately measure an agency's cybersecurity posture. The good news is that the recent Executive Order (EO) on cybersecurity, issued in May of 2021, can serve as a blueprint for what federal agencies should be doing to enhance their cybersecurity position. In particular, the EO places special emphasis on agencies implementing a zero-trust architecture, having holistic visibility across one's IT infrastructure, implementing secure guidelines in cloud computing environments, focusing on protecting high-value data and system assets, and dealing with supply chain issues. The EO can serve as the means to more accurately grade an agency's cybersecurity posture.

Longer-term (within the next few years), I would also like to see the following changes:

- **Add an "IT Workforce" Category** – While more challenging to measure, there is hardly a more important category regarding the ability of an agency to properly manage IT. Having the proper IT positions defined and having them filled with individuals that have the requisite knowledge, skills, and abilities (KSAs) is critical to success in any IT organization.

- **Add a "Customer Satisfaction" Category** – IT organizations have customers. A core measure for all agency support organizations should be customer satisfaction. It would be a best practice to administer a standard customer satisfaction survey to all agencies so this category can be added to the FITARA Scorecard.

5. As we look to update the FITARA cybersecurity metric, how can Congress quantify and continuously monitor agency cybersecurity risk?

Answer: It was appropriate that a cybersecurity category was added to the Scorecard, as cybersecurity is an essential part of a CIO's responsibilities. However, the existing FISMA measures (even with the modifications to the law made in 2014) along with the cybersecurity cross-agency priority (CAP) goals do not address the full scope of an agency's cybersecurity posture. For instance, agencies should emphasize effectively measuring cybersecurity risks associated with cloud deployments, moving beyond static compliance-based checklists.

Below is a list of additional items that can be measured that can support Congress being able to quantify and continuously monitor an agency's cybersecurity risk:

- Meeting all the Cybersecurity Executive Order (EO) dates and requirements.
- Meeting DHS and NSA Binding Operational Directives.
- Meeting DHS and NSA Emergency Directives.
- Fulfilling all Zero-Trust implementation requirements (including implementation of enterprise multi-factor authentication (MFA) and secure access service edge (SASE) solutions).
- Being responsive to cybersecurity-related audits (meeting deadlines to support IG and GAO work and implementing recommendations per the agreed dates).
- Establishing baseline levels of risk aligned to the OMB's FY 2021-2022 FISMA guidance. (Specifically, the new data elements in Appendix A related to scanning internet-accessible addresses and segments of Federal civilian agency systems for vulnerabilities on an ongoing basis.)

6. 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?

Answer: I don't believe there can be an effective Scorecard cybersecurity metric that only includes public data. For example, an agency meeting DHS Binding Operational Directives and Emergency Directives is essential and can be measured. But if an agency does not meet an Emergency Directive, it signals a potential vulnerability in an agency's cybersecurity posture

that definitely should not be made public. In such situations, GAO can give a composite grade to the totality of an agency's cybersecurity sub-measures that are non-public, and only that composite grade is reported. This composite grade for non-public data is then combined with other cybersecurity measures (such as the agency FISMA score) to arrive at an overall cybersecurity grade. While not as transparent as today's grading, such an approach still enables those interested in the Scorecard to understand how an agency's cybersecurity grade was calculated.

7. How can the Subcommittee effectively measure customer experience, including agency adoption of user- and customer-centric design and implementation processes?

Answer: While measures can be used to attempt to grade user- and customer-centric design and implementation processes, it will be difficult to get data that is consistent across all agencies—there is such wide variation in how agencies serve their users and customers. How agencies go about serving their customers varies significantly. For instance, some agencies have a highly citizen-facing mission and set of interactions (like the Social Security Administration - SSA), while others interact more with other organizations and government agencies (like the Environmental Protection Agency – EPA).

I recommend Congress consider working with GAO and the Administration to develop a standard customer satisfaction survey that all agencies could administer. This is a best practice in the private sector, and it would orient agency IT organizations to focus on the users and customers of their services. The survey would measure a number of facets of IT delivery, including day-to-day operations support as well as addressing issues and even responding to outages. But an essential part of the survey would ask customers to rate their IT organization on how well they are working with customers to ensure solutions are designed to best support customer needs and address agency goals and objectives.

8. How can the Subcommittee measure customer experience in a way that accounts for interactions with the federal government that cross agency boundaries or fluctuate over time (e.g., after losing a job or starting a family)?

Answer: Measuring customer experience is problematic when an agency is heavily reliant on another agency or agencies to provide a service to a customer. However, ultimately, the agency dealing directly with the customer (the lead agency) needs to take overall responsibility for the service provided to that customer. Suppose another agency's services are negatively impacting the customer service capabilities of the lead agency. In that case, it is incumbent on the lead agency to address that issue with the other agency.

As to how to measure customer experience in such a situation, I return to the recommendation of their being a customer satisfaction survey used to grade agencies on customer experience. If I am a citizen dealing with a lead agency, I should not need to know if other agencies are involved in providing me the requested service—it would be best if, as a customer, I did not need to deal with such complexity. Measuring customer satisfaction gives agencies an incentive to work to simplify the interactions with the customer, forcing agencies to better cooperate in situations in which a service comprises elements provided by multiple agencies.

9. **A key provision of the FITARA law requires agencies to provide the Office of Management and Budget with a data center inventory, a strategy for consolidating and optimizing the data centers, and quarterly updates on progress made. Given that all agencies received an "A" in this category of the FITARA 13.0 Scorecard, what might the next iteration of this metric look like?**

Answer: The data center optimization category has been a resounding success. Congress can now evolve data center consolidation to a more general "IT Infrastructure" category by capturing additional measures of agencies properly leveraging cloud computing, along with modernizing their networking infrastructures. Evolving this category will require the development of a cloud computing measure, which should focus on how well an agency is implementing the use of cloud computing as an enterprise capability, working to ensure it does not perpetuate additional stovepipes. A cloud computing measure could consist of the following sub-measures:

- Cloud computing is an integral part of the agency's IT strategic plan and enterprise architecture.
- Policies and processes are in place to assess all agency systems and applications for optimal use of IT infrastructure—whether in a data center or in the cloud.
- Adoption of formal Cloud Financial Operations concepts to optimize the use of the cloud for an agency.
- Contract vehicles in place that enable an agency to rapidly turn up FedRAMP-approved cloud services for agency use.
- The agency has a DevSecOps environment in place on a FedRAMP-approve cloud service.
- Demonstrated success in moving legacy applications from a data center to the cloud.
- Meeting the agency's EA documented transition strategy in migration to cloud services.

In terms of network modernization, Congress has already added to the Scorecard the migration to the GSA Enterprise Infrastructure Solutions (EIS) contract to modernize agency networking capabilities.

10. 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?

Answer: My answer to question 9 above addresses this question as well. I add that evolving to an "IT Infrastructure" category is not just about moving to the cloud. It involves optimizating the agency's infrastructure to best support its systems and applications. As such, the measures regarding data center optimization should remain, supplanted with measures addressing cloud computing and modernizing an agency's network infrastructure.

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

Answer: Regarding **IT modernization**, I recommend creating two categories to measure how well an agency plans for IT modernization, and then delivers on such modernization through the delivery of IT programs.

The "IT Modernization Planning" Category – Meaningful IT modernization starts with good planning and support by agency leadership. Hence, this category should reflect the maturity of an agency's planning function and enterprise architecture. In terms of planning, the agency should have a strategy that recognizes the importance of IT modernization and the retirement of legacy IT systems, with specific IT modernization objectives included in the agency's strategic plan. These IT modernization objectives should be driven by agency mission program priorities and be integrated into agency budgets, performance plans, and measures.

Such IT modernization plans should be captured in and be supported by an agency's enterprise architecture (EA). An agency's EA should include the definition and use of functional portfolios, target "to-be" business, technical, and data architectures that drive modernization, and governance that effectively allocates requirements from the enterprise to a portfolio, and then to a program or project for implementation. An agency's EA transition strategy should capture all of this detail and be updated every year.

To measure this category, existing "best practices" for planning and managing IT could be used to create an IT Planning maturity model. Either GAO or agency IGs could then use this model to audit an agency's IT planning capability to arrive at a maturity score. Given the rigor needed for this measure, it would be appropriate to have it revisited once a year rather than every six months as with the existing measures.

Combine the "Incremental Delivery" and "Transparency and Risk Management" Categories into a broader "Delivery of IT Programs" Category – Good planning, while necessary, is certainly not sufficient. Agency IT modernization occurs through the successful delivery of IT programs and projects. As such, there should be a category that measures the maturity of agencies in being able to manage such programs and projects. Such a measure would ultimately include the compilation of agency measures in the following sub-categories:

- Demonstrated use of appropriate program and project management disciplines.
- Professional development approaches to develop staff to fill critical roles in a program management office (PMO).
- A comprehensive approach to stakeholder engagement and program governance.
- Development and use of a systems development life-cycle (SDLC) that an agency can readily tailor for all types of IT programs.
- Commitment to incremental delivery and demonstrated use of Agile and DevOps techniques in programs, when appropriate.
- Proper and timely program status reporting, including an agency publishing data on the IT Dashboard.

While this measure may appear complex, there are well-understood and documented best practices in each of these sub-categories that can be measured to arrive at a composite grade regarding how well a government agency can manage its IT programs. Like the recommendation above on IT Modernization Planning, this measure would require an IG to annually audit an agency's practices.

For **IT workforce** planning, I recommend Congress develop a measure for the Scorecard. The measure could be created by combining the following elements:

- The agency CIO, partnering with the agency CHCO, has developed a set of competency models for the critical positions in the IT organization (these models include the knowledge, skills, and abilities (KSAs) for each key position along with expected behaviors for the position).
- The agency, based on these competency models, has developed career development paths for the more senior IT positions, with such development paths outlining approaches for developing the needed KSAs, including formal training, work assignments, and mentoring.
- All IT staff in the agency have, as part of their annual review process, formal individual development plans (IDPs) that support an individual in their career aspirations over at least a five-year period. Many of the IDPs would leverage the use of KSAs from an agency's position competency models and associated career development paths.
- The agency has a current IT workforce plan in place, showing where the agency has current workforce talent gaps, along with projections of gaps over a three-year period.

This plan should outline employee development and recruiting needs to address the agency talent gaps over the three years.

- The agency has established a robust training and development program to support IT workers in meeting their objectives as detailed in their IDP.
- The agency demonstrates it has a comprehensive recruiting approach to address critical IT workforce gaps, using all of its special authorities and government-wide recruitment efforts to be able to recruit individuals into IT positions.

With this level of workforce planning and development, agencies can build, over time, a capable IT organization needed for sustained success. Additional data would need to be collected and reported by agencies to implement such a measure. But such a measure could be in place within a year to 18 months with a sustained focus on establishing the process for collecting the data.

Questions for Mr. Richard A. Spires
Questions from Rep. Jody Hice

Subcommittee on Government Operations

January 20, 2022, Hearing: "FITARA 13.0

1. **FITARA provides a framework to reform how federal agencies purchase and manage their information technology assets. During your time in the government, what were the biggest challenges you faced while working on FITARA implementation? Was FITARA an effective tool in your effort to drive change?**

   Answer: I served as the CIO of IRS from 2006 to 2008 and as the CIO of DHS from 2009 to 2013. Both of my tenures of being a CIO in government pre-dated the enactment of FITARA. Hence, I don't have first-hand experience regarding the implementation of FITARA. But let me address what I believe to be the spirit of the question. When I became the IRS CIO, I reported directly to the leadership of the organization, the Commissioner and the Deputy Commissioner for Operations Support. I was able to build solid relationships with the Commissioner and Deputy Commissioner, and I was a true partner with the business unit leaders. I worked with them to address how IT could best be used to support desired business outcomes, while also balancing the need to address long-term IT modernization and cybersecurity concerns. That model worked well, and we were able to advance important initiatives for the IRS. In particular, I cite several major projects delivered during that time, including Modernized e-File and the Integrated Financial System (IFS). And we did foundational work, particularly in improving the IRS' ability to manage IT programs and projects. That positioned the IRS to establish a program that successfully implemented the tax-related components of the Affordable Care Act (ACA or Obamacare) when that Act was passed in 2010. This foundational work was also instrumental in enabling the IRS to come off the GAO High-Risk List for its IT modernization efforts in 2013.

   I contrast my IRS experience to that of DHS. At DHS, I reported to the Undersecretary for Management, who in turn reported to the DHS Secretary and Deputy Secretary. I am proud of the work I did at DHS for nearly four years as CIO, and we did make progress in a number of areas. But so much more could have been accomplished. I never built a strong relationship with the Secretary and Deputy Secretary, and I never felt I was a partner with the business unit leaders, those individuals leading the Components of DHS (e.g., FEMA, TSA, etc.). As such, I could never fully do the job I was hired for, and I believe that DHS suffered for it. Hence, when the discussion began in Congress on passing a law to address federal IT management and acquisition, I was an enthusiastic supporter. I provided input to Congressional staff as they worked with co-sponsors Rep. Connolly and Rep. Issa to craft what became FITARA. My

input reflected on the differences between my experiences at IRS and DHS, focusing on the need to have that strong partnership between the agency business unit leaders and the CIO. The tenets of FITARA, properly leveraged by a capable CIO and staff, empower the CIO to become that partner with the agency business unit leaders.

2. **As the Data Center Optimization Initiative paves the way for movement into cloud infrastructure, platforms, and software, are there opportunities to measure the efficiencies gained through investments in cloud computing solutions?**

    a. **What are some of the unique challenges in maintaining such inventories and managing associated costs?**

    b. **How should agencies track and manage the software applications they have moved into the cloud?**

    Answer: Agencies, through proper planning, should be taking advantage of cloud computing to make their IT infrastructures not only more modern but also more efficient. Just doing a lift and shift of applications from an existing data center to the cloud benefits an agency but most likely will not result in cost efficiencies. Conducting the proper analysis and leveraging technologies like virtualization can enable agencies to take full advantage of the cloud. The private sector is well ahead of most government agencies in the adoption and optimization of using cloud capabilities. Recently, a discipline called Cloud Financial Operations (FinOps) has arisen that works to codify best practices in using the cloud. And the FinOps Foundation (https://www.finops.org/introduction/what-is-finops/) is working with all types of organizations (including federal government agencies) to support them in migrating to the cloud and getting the most from their use of the cloud. I expand upon this question by listing potential sub-measures to create a cloud computing measure in answering question 7 below.

    Answer to parts a and b: Modern cloud computing platforms provide advanced tools to measure aspects of a customer's use of the cloud, including application tracking, usage, and costs. The recommendations of best practices provided by the FinOps Foundation can help agencies best manage those applications to ensure they are efficiently using their cloud services.

3. **This Subcommittee has repeatedly expressed concerns about federal agencies' ability to transition to the Enterprise Infrastructure Solutions (EIS) program by the May 2023 deadline. The December 2021 FITARA Scorecard identifies 15 agencies that failed to meet the March 2022 milestone.**

a. **What are some reasons why agencies may not meet the 2023 deadline, and what happens if they do not?**

b. **What practical benefits does the EIS program provide to agency operations, missions, and cybersecurity? In other words, what are agencies missing out on by not taking full advantage of EIS?**

c. **What options do agencies have to maintain operations while they continue to transition beyond the deadline?**

d. **If the EIS transition is ultimately a failure, what other IT and government- wide reform initiatives does this put at risk?**

Answer to part a: Regarding the low marks for transitioning from Networx to EIS, it is a problem of both priorities and OCIO workforce capabilities. A CIO at an agency has probably a dozen or more "high priority" items to address. This includes making sure existing systems perform adequately to support the mission, and addressing the demand for new functionality to improve mission effectiveness (these should be the highest priorities). But then layer on the cybersecurity requirements, all the OBM reporting, dealing with audits from an IG and GAO, and dealing with the Hill. So, while it looks like moving to EIS should be a high priority, in reality, it is one of a number of high priorities that a CIO and their staff are constantly dealing with.

But this points to the real underlying reason for the delay in transitioning off of Networx – most OCIO organizations are not staffed nor have the talent to deal with all of these high-priority items. They constantly have to decide what they must focus on and what can be slid till later. And while transitioning off of Networx does have high visibility, it probably still does not supplant new mission functionality a Head of Agency wants to be delivered. Agencies need to understand and adequately fund OCIO organizations to build a strong team that can address all of these high-priority items effectively.

Interestingly, since the Subcommittee issued these questions, GSA has announced it intends to issue a continuation of services (CoS) clause for the Networx contracts, which has the effect of giving agencies one more year to transition off of Networx. The reality is that GSA is not likely to leave agencies in a lurch in which Networx services are discontinued before all agencies fully migrate to EIS—the impact on mission delivery for agencies would be too severe.

Answer to part b: The EIS contract structure and procurement approach was designed with significant input from government agencies and the private sector. ACT-IAC's Institute for Innovation prepared an EIS Case Study published in June 2020. The following describes the benefits of EIS over the existing Networx contracts.

> EIS provides for a lower-cost model with a modern telecommunications infrastructure. EIS introduces new capabilities and outlines a technology path toward modernization by offering new and emerging technologies. These technologies enable an agency to take advantage of combining services such as Ethernet, Voice over IP, and SD-WAN into a single delivery method over a modern infrastructure, enabling transformation to future technologies. EIS encompasses 37 service categories, including both legacy and modern technologies and increased core-based statistical area (CBSA) to 929 geographic areas defined by OMB. This logical grouping by service categories and the EIS award criteria promoted increased vendor participation and expanded competition. Furthermore, EIS's structure and guidance from GSA make it easier for agencies to move away from a "winner take all" bidding strategy. EIS also offers diverse and creative agency-specific solutions, offers prices well below benchmarks for common services, and provides agencies with the ability to define mission-critical services transition planning.

Answer to part c: As stated above, the reality is that GSA is not likely to leave agencies in a lurch in which Networx services are discontinued before all agencies fully migrate to EIS—the impact to mission delivery for agencies would be too severe.

Answer to part d: Given the approach GSA is taking by extending the transition by one year, EIS will not be a failure in the sense of agencies not being able to fully transition to it. Certainly, some agencies that lag in the transition will sacrifice some of the benefits of EIS. Eventually, all agencies will migrate from Networx to EIS.

4. **Can you describe the burden placed on federal agencies due to the semiannual FITARA cadence? Does this frequency impact the accuracy of the picture presented to the Subcommittee of the government's IT posture?**

Answer: Since the FITARA Scorecard measures are currently based on data already being collected and reported by agencies, the burden on agencies from the semiannual FITARA cadence is relatively low. I do not believe this frequency impacts the accuracy of the picture presented to the Subcommittee.

However, I have heard frustration from some CIOs that six months is a relatively short time. In many instances, it can take much longer for an improvement initiative in an agency to reflect in a higher grade in a category. It can appear that there is little to no progress being made in a category when behind the scenes, much is being done—it has not yet been reflected in the data that can lead to a higher score.

As I have testified, for several of the new categories I am recommending (such as for "IT Modernization Planning" and "Delivery of IT Programs), changes to the grade be made annually, as opposed to six months. This is mainly due to an IG needing to audit an agency to determine the grade, but it also reflects the complexity and time required for agencies to improve in these categories.

5. **Given your prior government experience, what are your thoughts on how the National Cyber Director could complement federal agencies' efforts to strengthen their cybersecurity posture? Be as specific as you can.**

Answer: As a new position, the National Cyber Director's role has few formal powers and is not yet well-defined. Positively, the first National Cyber Director, Chris Inglis, has a deep understanding of the federal government and working in cybersecurity at an agency level, given his 28 years spent at the National Security Agency (NSA). He is a good choice for the position, as he works to assess how he and his office can add value in supporting federal government agencies.

Given my prior government experience, below is the list of activities the National Cyber Director can undertake that would best complement federal agencies' efforts to strengthen their cybersecurity posture:

- Review agency cybersecurity plans and budget requests and provide feedback to agencies on:
    - Appropriateness of the agency cybersecurity plan, citing gaps and inefficiencies as well as areas that should merit additional investment
    - Budget requests, regarding whether the budget is aligned with the cybersecurity plan and where additional or redirected funding should be directed
- Work with OMB (the federal CIO and CISO) and DHS' CISA on federal-wide cybersecurity policy, to include input on approaches to assess agency cybersecurity maturity, the data to be collected from agencies, and how best to provide real-time monitoring of agencies' cybersecurity posture.
- Be an informal advisor to agency heads, CIOs, and CISOs to provide advice and feedback on addressing cybersecurity issues.
- Work with GAO and agency IGs on improving how audits of agency cybersecurity are conducted.

- When a major breach affecting one or more federal agencies does occur, advise the Office of the President, OMB leadership, and agency leadership on appropriate actions to take, both to recover from the breach but also on how to limit the probability of such breaches to occur in the future.

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?

Answer: There are certainly legacy systems in federal agencies that should be retired and replaced. Some of the reasons agencies should replace specific legacy systems include: an inability for the system to support new mission requirements; the system is using unsupported software platforms, such as operating systems or databases that cannot be upgraded; or the system has significant cybersecurity vulnerabilities that cannot be addressed. But there are many legacy systems in agencies that meet mission needs, can be maintained, and do not create undue cybersecurity risk. Thus legacy system planning, as part of an agency's IT modernization plan and captured as part of its enterprise architecture (EA), is crucial for an agency. That is why I am recommending that a new category, called "IT Modernization Planning," be added to the Scorecard. This category should reflect the maturity and focus on IT modernization within the agency's planning function and enterprise architecture. To measure this category, existing "best practices" for planning and managing IT could be used by either GAO or agency IGs to audit an agency's IT planning capability to arrive at an IT Planning maturity grade.

7. FedRAMP is a crucial part to ensuring security as more and more agencies move to the cloud. What kinds of metrics could we use to track agencies' progress in leveraging FedRAMP-approved cloud technology solutions?

Answer: Congress can evolve data center consolidation to a more general "IT Infrastructure" category by capturing additional measures of agencies properly leveraging cloud computing, along with modernizing their networking infrastructures. Evolving this category will require the development of a cloud computing measure, which should include how well an agency is implementing the use of cloud computing as an enterprise capability, working to ensure it does not perpetuate additional stovepipes. In particular, a cloud computing measure could consist of the following sub-measures:

- Cloud computing is an integral part of the agency's IT strategic plan and enterprise architecture.

- Policies and processes are in place to assess all agency systems and applications for optimal use of IT infrastructure—whether in a data center or in the cloud.
- Adoption of formal Cloud Financial Operations concepts to optimize the use of the cloud for an agency.
- Contract vehicles in place that enable an agency to rapidly turn up FedRAMP-approved cloud services for agency use.
- The agency has a DevSecOps environment in place on a FedRAMP-approve cloud service.
- Demonstrated success in moving legacy applications from a data center to the cloud.
- Meeting the agency's EA documented transition strategy in migration to cloud services.

In terms of network modernization, Congress has already added to the Scorecard the migration to the GSA Enterprise Infrastructure Solutions (EIS) contract to modernize agency networking capabilities.

8. **In the last couple of years, the digital interaction of Americans with the federal government has increased and therefore customer service and citizen experience have become critical.**

    a. **Is this an important metric to identify and include in the FITARA Scorecard?**

    b. **If so, what kind of data would we need, and how could we incorporate customer experience into future FITARA Scorecards?**

Answer: While measures can be used to attempt to grade user- and customer-centric design and implementation processes, it will be difficult to get data that is consistent across all agencies—there is such wide variation in how agencies serve their users and customers. How agencies go about serving their customers varies significantly. For instance, some agencies have a highly citizen-facing mission and set of interactions (like the Social Security Administration - SSA), while others interact more with other organizations and government agencies (like the Environmental Protection Agency – EPA).

I recommend Congress consider working with GAO and the Administration to develop a standard customer satisfaction survey that all agencies could administer. This is a best practice in the private sector, and it would orient agency IT organizations to focus on the users and customers of their services. The survey would measure a number of facets of IT delivery, including day-to-day operations support as well as addressing issues and even responding to outages. But an essential part of the survey would ask customers to rate their IT organization on how well they are working with customers to ensure solutions are designed to best support customer needs and address agency goals and objectives

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.**

    1. **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?**

    2. **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?**

    Answer: As I describe in answer to question 8 above, I think overall customer satisfaction, as measured through a standard survey instrument, is a more practical approach to measuring customer experience. Below are a few of the complexities, specific to the usability and performance of public-facing websites, in measuring specific customer experience metrics:

    - Website design "best practices" are evolving rapidly, making it difficult to keep such metrics current.

    - Most large agencies have numerous public-facing websites (when I served at DHS, we had hundreds), and one would have to measure each website and arrive at a composite score for an agency. But many of these websites have relatively few customers, while typically, a small number of an agency's websites serve the large majority of customers. How does one construct a metric to take into account this reality?

    - While upgrading a specific website is helpful, I have found that often looking from a broader perspective can provide more insight and opportunities to improve customer experience. Such a perspective may lead an agency to consolidate websites, leverage capabilities from multiple agencies in a single platform, and offer customers alternative digital capabilities, like a mobile app.

    Based on these observations, I do not recommend using specific customer experience metrics as a FITARA Scorecard category.

10. **Workforce needs are rapidly changing as agencies continue to modernize. Should any update to the FITARA Scorecard capture agency investments in workforce, such as**

upskilling and retraining, partnerships with the private sector to augment workforce shortages, or the use of new authorities to bring in the needed talent?

Answer: I do recommend that Congress develop a workforce measure for the Scorecard. The measure could be created by combining the following elements:

- The agency CIO, partnering with the agency CHCO, has developed a set of competency models for the critical positions in the IT organization (these models include the knowledge, skills, and abilities (KSAs) for each key position along with expected behaviors for the position).
- The agency, based on these competency models, has developed career development paths for the more senior IT positions, with such development paths outlining approaches for developing the needed KSAs, including formal training, work assignments, and mentoring.
- All IT staff in the agency have, as part of their annual review process, formal individual development plans (IDPs) that support an individual in their career aspirations over at least a five-year period. Many of the IDPs would leverage the use of KSAs from an agency's position competency models and associated career development paths.
- The agency has a current IT workforce plan in place, showing where the agency has current workforce talent gaps, along with projections of gaps over a three-year period. This plan should outline employee development and recruiting needs to address the agency talent gaps over the three years.
- The agency has established a robust training and development program to support IT workers in meeting their objectives as detailed in their IDP.
- The agency demonstrates it has a comprehensive recruiting approach to address critical IT workforce gaps, using all of its special authorities and government-wide recruitment efforts to be able to recruit individuals into IT positions.

Only with this level of workforce planning and development can agencies build, over time, a capable IT organization needed for sustained success. Additional data would need to be collected and reported by agencies to implement such a measure. But such a measure could be in place within a year to 18 months with a sustained focus on establishing the process for collecting the data.

11. Over the last three years, there have been discussions – and in some cases reductions[2] – in the amount of information shared as part of the IT Dashboard. Since this information is used to inform portions of the FITARA Scorecard, do you think we are capturing the

[2] *OMB's IT Dashboard to Scale Back Data on Federal IT Spending*, Bloomberg Government (Apr. 2, 2019) (online at https://about.bgov.com/news/ombs-itdashboard-to-scale-back-data-on-federal-it-spending/).

right information on major IT investments? Do we need to change or update the information we collect on major IT investments to better reflect cybersecurity, customer experience, and modernization?

Answer: In the recommendations I make on evolving the Scorecard, there would be new data reporting requirements. In particular, these are the reporting requirements that would be most helpful providing robust oversight of major IT investments:

Data elements for an **"IT Modernization Planning" Category**:

- The agency should have a strategy that recognizes the importance of IT modernization and the retirement of legacy IT systems, with specific IT modernization objectives included in the agency's strategic plan.
- These IT modernization objectives should be driven by agency mission program priorities and be integrated into agency budgets, performance plans, and measures.
- Such IT modernization plans should be captured in and be supported by an agency's enterprise architecture (EA).
- An agency's EA should include the definition and use of functional portfolios, target "to-be" business, technical, and data architectures that drive modernization, and governance that effectively allocates requirements from enterprise, to portfolio, to program or project for implementation.
- Such planning should include an analysis of legacy systems, addressing those systems to be retired and how other existing or new systems will handle such functionality.
- This planning should be captured in an agency EA transition strategy that is aligned with the agency strategic plan and is tracked and updated annually.

Data elements for a **"Delivery of IT Programs" Category**:

- Demonstrated use of appropriate program and project management disciplines.
- Professional development approaches to develop staff to fill critical roles in a program management office (PMO).
- A comprehensive approach to stakeholder engagement and program governance.
- Development and use of a systems development life-cycle (SDLC) that an agency can readily tailor for all types of IT programs.
- Commitment to incremental delivery and demonstrated use of Agile and DevOps techniques in programs, when appropriate.
- Proper and timely program status reporting.

Given that some of these measures would require an IG or GAO to audit an agency to determine a grade in a category, it would make sense to move those categories (to include both the "IT Modernization Planning" and "Delivery of IT Programs") to a yearly update, rather than every six months.