**Dave Powner, MITRE, responses**

**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?**

Given that most of the data used to grade agencies comes from self-reported data to OMB, agencies can overstate progress. As an example, the incremental development (CIO enhancements) score is calculated based on agency submissions if their projects plan to deliver in 6-month increments. GAO reported in 2018 that their data showed less projects planning to deliver in 6-month increments than what was self-reported. I do not believe that this overstated reporting is resulting in significant grade inflation; however, there will always be this possibility with self-reported data. The solution is spot checks on the self-reported data with GAO reviews to keep the reporting accurate and honest. This challenge will not go away as the scorecard evolves, but the key is focusing on the right management areas needing attention – this will drive needed change even if some overstating of the data remains.

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?**

Consistent with my written statement and testimony, there are five broad categories where additional data reporting requirements would greatly help federal IT management. These are cybersecurity, workforce, legacy modernization, budgeting, and infrastructure. As an example, relevant cyber metrics associated with implementing zero trust strategies – such as the percentage of applications using multi-factor authentication or the percentage of the agency that has deployed endpoint detection and response (EDR) tools consistent the Department of Homeland Security's technical requirements – should be on the table for consideration. Regarding legacy modernization, agencies could be required to report all acquisitions that have hardware and software that is two versions or more older, or any hardware or software that is or will soon no longer be supported by the vendor. Also, another reporting metric could be legacy applications that contain more than five languages (as MITRE research on this topic shows that systems with five or more languages have significant costs to maintain, as well as being more vulnerable to security breaches). Agencies could then use the IT Dashboard to report the status of major IT acquisitions that address/replace our most vulnerable and difficult to maintain legacy systems.

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

FITARA has been successful in enhancing CIO authorities associated with approving IT budgets, certifying IT acquisitions to deliver in smaller increments, and approving IT contracts. It has also greatly enhanced the federal government's management of inefficient data centers and duplicative business systems. The next evolution of FITARA should build off these successes by enhancing:

- IT budgeting (including OMB's budget guidance) by requiring the use of the Technology Business Management (TBM) process
- IT acquisitions by focusing attention on the most mission critical acquisitions that help to enhance agency performance and address our legacy systems' challenge
- The training and use of IT cadres in FITARA by focusing holistically on the workforce, and requiring and supporting innovative recruiting, retaining, and training that incorporates best practices from the U.S. Digital Service and GSA's 18F
- Cybersecurity metrics that are consistent with industry measures and aligned with the revisions to the Federal Information Security Management Act (FISMA)
- Federal agencies' continued migration to cloud services

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

The workforce focus is clearly missing. Additionally, these four categories on the scorecard need to be updated:

- The dashboard category should focus less on risk acknowledgment and more on the status of the top acquisitions that address agencies' technology obsolescence and enhances mission performance and the citizens' experience obtaining government services.
- The MGT category should be expanded to a broader budgeting category and include TBM.
- The EIS category should be expanded to a broader Infrastructure category and include cloud migration efforts.
- The cyber category should be updated with metrics used by CISOs and industry and include supply change risk management.

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

The metrics used by Congress need to address the most pressing cyber risks. Focusing these metrics on the Administration's cybersecurity executive order, the zero trust policy, supply chain risk management best practices, and those metrics used by CISOs and industry will position Congress to do just that. OMB is currently adjusting the cybersecurity CAP goal metrics used by this Committee. Having input and direction from the National Cybersecurity Director and the Federal Chief Information Security Officer will be an essential step to determining a prioritized set of metrics. Lastly, having a collective team approach from both the Congress and these key executives at EOP and OMB will position our nation to focus on the right measures to best secure our nation's data and systems.

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?**

The Subcommittee should strongly consider metrics that are both public and non-public due to their sensitivity. Publishing an overall grade is fine, but the public does not need to know all the details of what went into the grade. This approach can hold agencies more accountable with a combination of open and closed meetings.

Dave Powner, MITRE, responses

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

Given the Administration's focus on customer experience with the Executive Order and the prioritization CX has in the President's Management Agenda, the Subcommittee should get access to the data that the Administration is using to measure customer experience and use this as a starting point. There are several options to measure CX. One measure would be a customer survey administered by each agency (the government could partner here with a firm that already does this type of survey research). Another option is to measure an agencies' CX maturity by having agencies report to OMB on key practices (human centric design, root cause analyses of customer challenges, use of data analytics, evidence-based decision making, use of technology to address challenges).

From a FITARA scorecard perspective, IT acquisitions that enhance mission performance and the customer or citizen experience can be used by the Subcommittee to measure improved customer experiences. Identifying these acquisitions and tracking their progress on the IT Dashboard will ensure that technology (e.g., artificial intelligence applications, platforms to manage data, modernized benefit systems) is a key enabler to improving the customer experience.

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)?**

This is a great question, but likely too large a leap for the current FITARA scorecard, which takes an agency-specific snapshot of progress. Cross-agency customer experience tied to life events will need a systems view. The first step is to identify the cross-agency flow of delivering services at certain life events. The second step is learning what customers value at each stage and overall (and how different customer needs influence what matters), and which stages are the most critical in achieving successful customer outcomes. The third step is identifying what data (or combinations of data) are the most valuable in measuring how well the government is delivering what customers (and the public) value at each stage and for the overall outcome. MITRE has and continues to research this topic and we can arrange for detailed briefings to assist the Subcommittee on this topic.

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?**

Clearly this is likely the best success story that resulted from the FITARA scorecard. Bottomline, the federal government has made the initial transition to the cloud and saved at least $5 billion in the process. This category now needs to transition to a cloud migration/adoption measure. A good start on this category, similar to the data center approach, would be for OMB to require a cloud migration strategy and have agencies report on their implementation status. Such an approach could easily allow for a simple grade on implementation and would keep the focus on further cloud adoption.

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

See response to #9.

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

IT modernization will require both modernized infrastructure and applications to enhance mission performance. The scorecard should evolve to have an infrastructure category that includes the current EIS focus and a cloud adoption component. Legacy modernization should also replace the current Dashboard category and highlight the top three to five IT acquisitions that enhance mission performance and address our legacy system challenges (these top acquisitions would be prioritized from a detailed analysis of applications that are not using current hardware or software). The workforce category should grade how agencies identify their current IT and cyber workforce gaps and how they fill such gaps with their recruiting and training activities.

**Questions from Rep. Jody Hice**

**January 20, 2022, Hearing: "FITARA 13.0"**

1. **A specific recommendation in your testimony was to include an IT workforce category. We are all aware of the difficulty in hiring IT professionals with in-demand skills.**

   a. **Could you please provide the Subcommittee with more detail regarding the full spectrum of actions agencies should take to address workforce needs?**

First, agencies need to assess their IT and cyber workforce needs and compare this to staff that are currently onboard. These gaps then need to be pursued through the chief human capital officer's recruiting and hiring processes. While federal agencies face competition and challenges in hiring a technically skilled workforce, a structured effort that prioritizes these hires will help to close our current gaps. In the short-term, critical gaps can be strategically filled with Intergovernmental Personnel Act (IPA) assignments and where appropriate, contractors on a limited basis. Over the years, we have also seen some agencies address these needs by working with Congress and OPM on getting critical hiring authorities for these key technical positions. CIOs should be working with CHCOs to explore all these options.

   b. **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?**

Training, partnerships, and new authorities are all good options, but visibility and transparency into agencies' workforce needs will help to address this challenge. There are not consistently good gap assessments nor aggressive efforts to tackle the IT and cyber workforce gaps across the federal government. One way to approach this on the scorecard would be to assign Fs to all agencies that do not have a current workforce gap assessment, a C should be assigned if the assessment is complete, a B would be awarded if agencies have closed the gap by 10 percent, and an A could be assigned by closing the gap by a higher percentage.

2. **Your written testimony included incorporating a potential new FITARA Scorecard category regarding IT budgeting/funding.**

   **You wrote: This category should continue to include the underperforming working capital funds and incorporate Technology Business Management (TBM) methodology to better capture all IT costs and align them to the agency or citizen services they enable. In addition, agency IT budgets cannot remain relatively flat or receive only modest increases if we are to modernize to the extent needed and turn the corner on the 80 percent-plus being spent on legacy operations. Although the Technology Modernization Fund (TMF) has been helpful,**

**agencies cannot rely on this for future budgeting. Agency IT budgets need to better reflect the IT needs of agency CIOs and mission leaders.**
**Could you expand on this concept further by providing a description of current practices along with your vision of an improved methodology that incorporates TBM?**

As an example, an IT budgeting or funding category on the scorecard could look like this:

- 1/3 of the grade could be based on the current working capital grades that are currently assigned.
- 1/3 could be based on whether the agency has implemented TBM (Richard Spires written testimony presented an excellent way to approach this – no TBM = F, partial TBM = D, full TBM = C, with Bs and As assigned based on how the TBM data is used to manage.)
- 1/3 of the grade could be based on whether the IT budget is validated by both the CFO and CIO.

3. **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?**

Having detailed visibility into IT spending can be a challenge for federal agencies, but having accurate data on cloud instances and their associated costs should not be difficult if the acquisition, CFO, and CIO organizations are working together to manage this.

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

Software applications that have moved to the cloud should be managed with an applications rationalization process. Agencies should strategically identify applications across the organization so that they are constantly evaluated for modernization, retirement, or consolidation.

4. **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. Given your prior employment with GAO and experience producing the Scorecard, I would appreciate your responses to the following questions:**

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

I agree with Ms. Harris's comments at the hearing that this hasn't been a priority for federal agencies. There has not been enough of an incentive to transition to EIS, especially when GSA keeps extending the prior Networx contract. However, many agencies are missing out on the benefits of EIS. These include cost savings from increased supplier competition and price transparency, increased bandwidth, and new services that will allow for modernization and increased security features.

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?**

As stated above, the benefits include cost savings, increased bandwidth, and new services. Regarding cybersecurity, agencies that have transitioned to EIS are better positioned to implement zero trust approaches, an industry best practice and an Administration priority.

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

Agencies will continue to operate on the Networx while they transition.

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

Delaying this transition would slow modernization progress, including the priority to move to zero trust cybersecurity solutions.

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

   a. **If the 13 oversight hearings held by this Subcommittee thus far have not yet helped take federal IT off the GAO's high-risk list, what else needs to be done?**

To clarify, the cyber category was added at scorecard #6 in May 2018. The scorecard uses ten OMB cybersecurity metrics associated with authorization, personal access, and intrusion detection; and the latest FISMA Inspector General report. As my written statement highlights, these metrics and IG reports have not evolved along with the threats to our systems and data. Updating these metrics to be consistent with Executive Order 14028, zero trust tenets (e.g., multi-factor authentication), as well as metrics that CISOs and industry use will position the federal government to better manage our cybersecurity risks.

6. **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**.

The National Cyber Director can help agencies enhance their cybersecurity posture by establishing polices guiding cybersecurity budgeting, prioritization, and execution. Our cyber budgets do not always accurately reflect needs and the constantly evolving threats. Enhanced budget guidance and the resulting budgets could position agencies to address workforce shortfalls as well as technology investments. The National Cyber Director can also help agencies execute on these budgets by developing a prioritized set of cyber metrics consistent with the cybersecurity EO and zero trust strategy. These metrics could be reviewed periodically with the head of each agency and the National

Cyber Director. The National Cyber Director should not be viewed as just a strategy-setting/policy shop. It should also play an active role in ensuring that our cyber policies and priorities are executed.

7. **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?**

It is desperately needed. There needs to be a comprehensive risk assessment that looks at agencies' mission critical systems to identify those that are not operating with current hardware and software. These assessments should then be used to prioritize acquisition or modification plans for their top three to five legacy applications most in need of replacement These should then be highlighted on the IT Dashboard to track progress on these replacement efforts. In addition, the Federal CIO should have a prioritized list for the nation which is personally tracked by OMB.

8. **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?**

As part of the cloud adoption change recommended in my testimony, there could be a FEDRAMP focus that simply grades the percentage of cloud services that are FEDRAMP approved. The key to grading these areas is to make it easy to understand while driving intended outcomes/results. If the goal is to get agencies to procure more FEDRAMP-approved cloud offerings, such a metric would help to ensure the proper focus and progress.

9. **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?**

Modern technology clearly plays a significant role in improving the citizen experience in their interactions with government agencies. Migrating away from legacy applications and having a modern infrastructure that these applications ride on, has and will continue to enhance CX. As my written statement highlights, I believe the focus of the scorecard should be mission modernization and IT infrastructure. For example, IT acquisitions that enhance mission performance and the customer or citizen experience can be used by the Subcommittee to measure improved customer experiences. Identifying these acquisitions and tracking their progress on the IT Dashboard will ensure that technology (e.g., artificial intelligence applications, platforms to manage data, benefit systems) is a key enabler to improving the customer experience.

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

I believe the scorecard should stick to the cyber and technology categories that enhance the customer experience, but there are several options for measuring CX as a separate category. First, given the Administration's focus on customer experience with the Executive Order and the prioritization CX has in the President's Management Agenda, the Subcommittee should get access to the data that the Administration is using to measure customer experience and use this as a starting point. Other options including having agencies administer a CX survey or report to OMB on key practices (human centric design, root cause analyses of customer challenges, use of data analytics, evidence-based decision making, use of technology to address challenges).

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

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

The website modernization standards called for in the IDEA Act are clearly an important requirement and a critical step to improving the citizen experience. However, I would not have this as a standalone metric on the scorecard. It could be included in the mission modernization category that I recommended.

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

I do not have data on this topic.

11. **Over the last three years, there have been discussions – and in some cases reductions – 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 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?**

The IT Dashboard has been an effective tool for executive management and oversight over the years, but it could be greatly enhanced. An enhanced Dashboard could not only highlight what agencies are spending their IT dollars on, but provide even better insights into how those investments are performing with the red/yellow/green risk rating. Consistent with my written statement, the Dashboard should identify the top IT acquisitions that enhance mission performance and replace our most vulnerable legacy applications. It could also be used to more clearly report on our cloud investments and an agency's spending on cloud. Finally, it could highlight those cloud investments that are FEDRAMP-approved. There are many possibilities for improvement that could be tied to future scorecard approaches.