Questions for Mr. Richard A. Spires
Questions from Chairman Gerald E. Connolly

August 3, 2020, Hearing: "FITARA 10.0"

1. **During your time as Chief Information Officer (CIO) at the Internal Revenue Service (IRS) and the Department of Homeland Security (DHS), how did you see the CIO's role evolve through the implementation of the Federal Information Technology Acquisition Reform Act (FITARA) and the Scorecard?**

   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 the first-hand experience regarding implementation of FITARA and the scorecard that is asked in the question. But with that being stated, 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, working with them to address how IT could best be used to support desired business outcomes, while properly balancing the need to address long-term IT modernization and cybersecurity concerns. That model worked well and we were able to advance significantly important initiatives for the IRS. In particular, I cite a number of major projects that were delivered during that time, to include 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 of 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 was never able to build a strong relationship with the Secretary and Deputy Secretary, and never felt I was a partner with the business unit leaders, those individuals that were leading the Components of DHS (e.g., FEMA, TSA, etc.). As such, I never felt I could fully do the job I was hired for, and I believe that DHS, in terms of how IT could best support the mission, suffered for it. Hence, when there began to be discussion in Congress on passing a law to address federal IT management and acquisition, I was an enthusiastic supporter and 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, with a focus 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 CIO you led the IRS's Business Systems Modernization program, one of the largest and most complex IT modernization efforts ever pursued. How did FITARA help you direct this largescale IT modernization program?**

Answer: As I responded to in question number 1, FITARA was not in existence when I served at the IRS. But let me expand upon the general topic of IT modernization initiatives and the importance of FITARA to such initiatives. As I stated in my written testimony, we have significantly more work to do at many agencies to modernize our IT systems. But even if we had unlimited funds to invest in IT, the federal government would struggle because many of our agency IT organizations, even with the progress made during the past five years, still do not have the management maturity and skills to effectively deliver large-scale IT modernization.

Meaningful IT modernization starts with good planning and support by agency leadership. An agency should have strategies that recognize the importance of IT modernization and retirement of legacy IT systems, with specific IT modernization objectives included in the agency strategic plan. These IT modernization objectives should be driven by agency mission program priorities and be integrated into agency budgets and performance plans and measures. Further, such IT modernization plans should be captured in and be supported by an agency's enterprise architecture (EA). Included in an agency's EA should be 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. All of this should be captured in an agency EA transition strategy that is aligned with the agency strategic plan and is tracked and updated on a yearly basis.

Good planning, while necessary, is certainly not sufficient. Agency IT modernization occurs through the delivery of IT programs and projects, and below are key aspects needed to help ensure IT programs and projects are successful:

- 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)
- Comprehensive approach to stakeholder engagement and program governance
- Development and use of a systems development life-cycle (SDLC) that can be readily tailored 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.

In terms of both IT modernization planning and execution, we were able to make significant improvements while I was the IRS, in large part due to having the IRS Commissioner's support and having a strong partnership between the IRS business unit leaders and the leadership in the CIO's organization.

To support agencies to improve their planning and execution capabilities to deliver IT modernization, I recommended in my written testimony that we work to evolve the FITARA Scorecard to both capture elements of good planning for IT modernization along with the measuring an agency's ability to successfully deliver IT programs and projects.

3. **In 2015, you testified before the Senate Appropriations Committee about how while serving as CIO at IRS and DHS you felt the yearly Federal Information Security Management Act (FISMA) reports did not reflect the reality of the government's IT security posture. How can we update FISMA to enable agencies to improve their information security programs?**

Answer: While well-intentioned and appropriate for its time, FISMA skewed the approach for government IT information security. Originally enacted in 2002, it set a course for how IT security effectiveness has been measured in government. While there are some good components of the law, the unintended consequence is that it forced chief information security officers (CISOs) to look at the controls for individual systems when in reality, IT systems across the government were already becoming more interconnected and viewing systems in isolation did not reflect an agency's true enterprise security posture. Further, based on OMB guidance, FISMA was implemented during a period when the cyber-threat was still emerging and the evolution of technology hadn't yet recognized the necessity of a security development lifecycle. And furthermore, the law required the generation of paper-based reports, which diverted time, resources and personnel from effective security efforts. As the question states, at both IRS and then DHS, I was consistently reluctant to put my confidence in the yearly FISMA report since it did not reflect the reality of the true security posture of our overall IT environment. That can only be done by proper use of tools that continuously monitor the IT environment and are able to identify vulnerabilities in near-real time.

While upgrades to FISMA in 2014 addressed some of these shortcomings, I regularly hear from agency security personnel that still too much of the security work they do is compliance driven, and they are not able to effectively allocate resources to address cybersecurity vulnerabilities where it will do the most good for an agency. This points to the need for agencies to use an enterprise cybersecurity risk management framework to ensure agencies are

focusing on protecting their most sensitive data and critical systems. The good news is NIST has developed such a risk management framework, called the NIST Cybersecurity Framework (CSF), and its use by federal agencies was mandated by President Trump in his 2017 Executive Order on Cybersecurity.

Further, agencies should be driving to use modern security architectures. Now is the time for federal agencies to work to implement a Zero Trust security strategy. The legacy perimeter-based security strategy has been overcome by the advent of mobility, cloud computing, and insider threats. A Zero Trust security strategy is a proven 21st century approach that, when implemented properly, provides better protection at lower cost. The good news is that many government entities have elements of Zero Trust already deployed in their infrastructure, to include identity credential and access management (ICAM) solutions along with continuous monitoring.

Hence, FISMA should be updated to reflect the mandatory use of the NIST CSF. Further, the legislation should reflect the need for agencies to modernize their security architecture, moving to the use of a Zero Trust model. I would recommend that the updated FISMA establish tangible targets for Zero Trust implementation, such as "each agency shall implement at least one Zero Trust pilot by the end of fiscal year 2021 and achieve full Zero Trust capability throughout their enterprise by the end of fiscal year 2024."

And in lockstep, the cybersecurity category in the FITARA Scorecard should be revisited, starting with measuring whether an agency is properly executing the seven process steps of the NIST CSF and moving to modernize it security architecture. The evolution of the scorecard metric can take place irrespective of whether FISMA is updated.

4. **Do you think CIOs have been able to leverage FITARA to help them evolve their agencies' culture to be more amenable to making changes that will ultimately help improve IT management and performance?**

Answer: I do see evidence that many agencies have been able to evolve their cultures to being more amenable to making changes that will ultimately help improve IT management and performance. But as I stated in my written testimony, while the text of the legislation itself has been of aid, I believe it has been the oversight of Congress that has been the driving factor in making improvements. And I note that the passage of FITARA, and subsequent oversight efforts, particularly by this Subcommittee, have been handled in a bi-partisan and unified approach. That has made a significant positive difference in how seriously both President Obama's Administration and now President Trump's Administration have handled implementation of FITARA.

Yet, it is also the case, as evidenced by how agencies reacted to the pandemic, that we do have a more work to modernize our IT systems. It is my belief that even if we had unlimited funds to invest in IT, the federal government would struggle because many of our agency IT organizations still do not have the management maturity and skills to effectively deliver large-scale IT modernization. In 2015, the United States Government Accountability Office (GAO) placed the whole federal government on its High-Risk List for "Improving the Management of IT Acquisitions and Operations." In GAO's latest report on its High-Risk List, published in January 2019, GAO provides an update on this particular high-risk item. While GAO gives OMB credit for demonstrating leadership commitment to address weaknesses in management of IT acquisitions and operations, the report goes on to state the government has only partially met requirements in the capacity, monitoring, action plan, and demonstrated progress elements of this high-risk item. In the action plan element, GAO had recommended that 12 agencies identify and plan to modernize or replace legacy systems. As of December 2018, only 3 of the 12 agencies had implemented GAO's recommendation and made progress in planning to modernize their legacy systems. And even where I worked, at the IRS, the Treasury Inspector General for Tax Administration (TIGTA) just released a report (on August 19, 2020), stating "The IRS has not developed specific or long-term plans to address updating, replacing, or retiring most of its legacy systems."

Given the existing challenges in Federal IT, active, bi-partisan Congressional oversight is vital to continued progress. And given the success of the FITARA Scorecard over the past five years, the scorecard should continue as the means to measure agency progress over time. Yet the scorecard should evolve to address the continued challenges agencies face in IT modernization and in overall management of IT.

5. If you were the federal CIO, what would your top priorities be?

Answer: If I were serving as the federal CIO, I would focus on the following six priorities:

- ***Developing Comprehensive, yet Realistic, Agency IT Modernization Plans*** – As is stated by GAO in its latest High-Risk report, many agencies are not focused on the proper enterprise planning for IT modernization. As such, agencies conduct piecemeal modernization which, while of some value, continues to proliferate stovepipes, adds complexity, and makes the management of an agency's IT environment even more difficult. The Office of the Federal CIO would work with agencies to ensure they develop comprehensive IT modernization plans that are realistic given budget and talent constraints in the agency. Being realistic may mean that an agency has a modernization plan that may take between five and ten years to execute, but that is still much preferred over piecemeal plans that will never result in true enterprise modernization. And while IT modernization can itself result in lower operating costs and a better cybersecurity posture, IT

modernization planning really must start with agency mission improvement goals and objectives, and IT modernization programs and projects must address how such mission goals and objectives are being met, or at least advanced, through the successful delivery of those programs and projects. That is the only way to garner agency leadership support for sustained IT modernization.

- ***Improving Agencies Ability to Manage IT Programs and Projects*** – New capabilities delivered through IT modernization only happen with successful delivery of IT programs and projects. And while there is a lot of focus on program and project management, the GAO continues to keep the whole federal government on its High-Risk list for "Improving the Management of IT Acquisitions and Operations." Agencies need to work to mature their program and project management capabilities, with particular focus on the following:

    ◊ 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)
    ◊ Comprehensive approach to stakeholder engagement and program governance
    ◊ Development and use of a systems development life-cycle (SDLC) that can be readily tailored 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.

    The Office of the Federal CIO would work with agencies to ensure they were taking steps to mature these capabilities.

- ***Addressing Procurement Timeliness and the use of Strategic Sourcing and Category Management*** – One of the biggest frustrations I had as an agency CIO were the lead times necessary to get procurements completed so we could deliver new capabilities for our customers. It is an important element of improving agencies ability to manage IT programs and projects. The Office of Federal Procurement Policy (OFPP), partnering in particular with GSA, has made significant advancements in addressing this issue of timeliness, mainly through the use of strategic sourcing and category management approaches. If I were the federal CIO, I would extend that good work, partnering with OFPP, GSA, and other agencies to continue to advance the use of these vehicles and concepts for all IT purchasing. With the acceleration of advances in IT technologies and services, we need to reduce the time to complete procurements, while simultaneously continuing to work to ensure agencies are getting best value in their IT purchasing.

- ***Improving Agencies' Cybersecurity Posture*** – Cybersecurity breaches have become the biggest risk for many organizations, including government agencies. And across the federal government, we still have significant areas of vulnerability. If I were the federal CIO, I would focus on working with agencies to address the priorities I listed in the answer to

question 3 above, namely the use of an enterprise risk management framework (the NIST CSF) along the migration toward a modern security architecture, the use of a Zero Trust model. I should point out that in developing an IT modernization plan, an agency would use the NIST CSF to help determine the priorities for cybersecurity controls across the agency, and adhere to Zero Trust concepts in technical implementation. Hence, an agency's approach to improving its cybersecurity posture would be an integral part of its IT modernization plan.

- ***Addressing the IT Talent Gap*** – Across the federal government, the number of workers over 60 years old is almost double the number of those under 30. We are simply not attracting enough younger talent to government, and the problem is particularly acute in technology disciplines. Hence, many agencies struggle to even effectively oversee their technology contractors given the lack of technical talent in the agencies. We need to make the federal government a more attractive place to start your career, or even enter mid-career. As federal CIO, I would seek to partner with OPM and the federal CHCO Council on additional ways we can both attract and retain technologists in government. I entered government mid-career, and was very taken with the mission and scale of what I could do as a technical leader. We must find improved ways to market these opportunities. This is imperative if we are going to continue to improve agencies ability to leverage IT to the benefit of improving their mission execution.

- ***Improving Alignment across the Administration and with Congress*** – Having served as an agency CIO, I recognize the burden of reporting requirements on agencies, particularly from OMB. If I were federal CIO, I would work to lower reporting burden on agencies, and focus agency reporting on the most important aspects of improving their IT management. Likewise, I would hope to work with Congress to evolve the FITARA Scorecard, working to gain alignment of agency reporting with the reporting required to determine an agency grade via the FITARA Scorecard. Having such alignment of Administration IT priorities with how Congress is grading agencies would accelerate the adoption of IT management best practices across the federal government.

6. In your testimony you stated that "the improvement in grades on the FITARA Scorecard over time tells part of the story," could you speak to the other side of that story?

Answer: As I stated in my written testimony, there have been tangible improvements in federal IT over the past five years, to include:

- Greater use of strategic sourcing vehicles and enterprise licensing agreements, that for some of the larger agencies, save them hundreds of millions of dollars a year
- Significant consolidation of data centers, resulting in billions of dollars saved

- Improved management of IT programs through the use of incremental delivery methods, and now the burgeoning use of Agile and even DevOps methodologies
- Significant adoption of commercial cloud-based services, both for basic computing, but also software-as-a-service (SaaS), the use of commercial cloud-based software applications
- Improved CIO authorities with more CIOs reporting to the head or deputy head of agency, and CIOs having greater insight to and oversight of agency IT spending.

And a number of these improvements are reflected in the scorecard grades. However, I will reiterate that many agencies are struggling with many elements of managing IT. Perhaps most importantly, I don't see many agencies stepping up to address what it will take to truly modernize their IT environment, from the planning to improving their ability to manage IT programs and projects. To obtain the long-term value from IT for an agency, and to ensure its cybersecurity posture is sound, such modernization is critical.

7. As the FITARA Scorecard evolves, how can Congress ensure it still captures improvement at agencies over time?

Answer: In discussions regarding the scorecard, one will hear of the idea of retiring certain categories so new categories can be added, thus still keeping the scorecard relatively simple. Yet the existing measures are important to federal IT, and should not be retired. Many of the measures, in my recommendations, should evolve to capture a more comprehensive view of the IT management maturity within an agency. Let me provide two examples.

The use of enterprise licenses is critically important to ensure agencies are being cost efficient in providing IT services. I found at both IRS and DHS that there were significant savings to be found in continuing to pursue enterprise license agreements with major IT suppliers, for software, hardware, and IT services (such as cloud computing). Given the current measure for software licensing, I recommend this measure be revised to "raise the bar" so that agencies continue to explore how they can drive savings through improved supplier management practices, and the use of enterprise agreements and category management concepts. To continue to keep the scorecard simple, this revised licensing measure could then become an element of the portfolio review category, which focuses on the overall efficiency of IT (most notably focused on cost savings) within an agency.

As another example, I recommend evolving the "Managing Government Technology" category to a broader "IT Budget" category. This category should keep the element of an agency having an IT working capital fund. Yet, one of the issues that most federal government agencies face is not having good insight into the cost elements of the agency's IT budget. On a positive note, the federal government has adopted the Technology Business Management (TBM) taxonomy, which is an industry-standard taxonomy for categorizing IT costs, enabling agencies to capture IT cost detail and determine what it costs to deliver its IT services. With

such information, agencies are then able to benchmark themselves in the provision of commodity IT services, such as standard desktop applications, collaboration tools (to include e-mail), access services (such as remote access for employees), and basic compute and networking capabilities. Agencies should both understand the cost to provide such services, but also have insight to how they stack up, benchmarking themselves with other similar-sized agencies and private-sector corporations.

So, with an approach that enhances existing scorecard measures to provide a more comprehensive picture of the state of an agency's IT, it is possible to both evolve the scorecard, yet still have the ability to capture improvements at agencies over time.

8. What lessons can we glean from the pandemic about how we should measure agency progress in modernizing IT?

Answer: There are three lessons we should glean from the pandemic and how it affected federal IT:

- ***Exposing the Issues with Agency Legacy Systems*** – Agencies, over time, hone their processes to deal with the IT systems and those systems capabilities. But many legacy IT systems don't provide much agility when the environment changes. The pandemic exposed these weaknesses, particular for agencies that had to handle increased volumes and at times, changing business processes. Certainly, SBA had issues based on their legacy systems environment, but they were not alone. The Department of Veterans Affairs and the IRS also struggled based on systems issues. And while not directly federal government, many states had issues with their legacy unemployment claims systems. The lesson is that while agencies get by with legacy, out-dated IT systems in normal operations, they can struggle significantly when such systems are put under stress in crises. We should not, as a government, be complacent regarding the need to modernize many of these legacy systems.

- ***Recognizing the Importance of Collaboration Tools*** – If it was not evident before the pandemic, it certainly has shown us the value, and even necessity, of having modern collaboration platforms available to share information, hold virtual meetings, and conduct business with no one in a physical office. This pandemic is changing the way the office world works, and I don't expect we will be reverting to the previous model anytime soon, if ever. The lesson is that government agencies need to plan for this type of new working environment in their IT modernization plans.

- ***Celebrating the Resilience and Ingenuity of Federal Government Employees –*** While there is a tendency to focus on the negative aspects of the federal government's response to the pandemic, I wish to point out that agencies largely were able to convert to a new operating model, leverage online collaboration tools, and continue to work with little

diminished productivity. There was a lot of hard work, dedication, and ingenuity to make this happen, and it gives me a lot of hope for the future. We still have significant issues to overcome for agencies to effectively plan and manage IT. But with proper focus on addressing the most important issues, we can make very significant positive progress over the next five years.