

STATEMENT OF RICHARD A. SPIRES  
FORMER CHIEF INFORMATION OFFICER OF THE U.S. DEPARTMENT OF  
HOMELAND SECURITY AND THE INTERNAL REVENUE SERVICE

BEFORE THE  
SUBCOMMITTEE ON GOVERNMENT OPERATIONS  
OF THE  
HOUSE COMMITTEE ON OVERSIGHT AND REFORM  
JANUARY 20, 2022

Good morning Chairman Connolly, Ranking Member Hice, and members of the Subcommittee on Government Operations. I am honored to testify today on the Federal Information Technology Acquisition Reform Act (FITARA) and the FITARA Scorecard that Congress has issued over the past six years. Today, my testimony augments what I presented on FITARA and the use of the scorecard at a FITARA hearing held by this Subcommittee in August 2020. At that time, I presented my views with a forward look on Federal IT and recommendations to the Subcommittee on how best to evolve the scorecard. In this testimony, I refine those recommendations presenting my views on priorities for evolving the scorecard. I hope my testimony is of value to Congress as a means to help keep the FITARA Scorecard a valuable oversight tool.

Having served as the Chief Information Officer (CIO) of a major department (the U.S. Department of Homeland Security), as well as the CIO for a large bureau (the Internal Revenue Service in the U.S. Department of the Treasury), I had ample opportunity to experience the management dynamics inherent in federal government IT. I also had the honor to serve as the Vice-Chair of the Federal CIO Council for three years, working to help drive improvements in the management of IT across the federal government. When Congress was drafting the FITARA legislation, I served as DHS CIO and provided both input and testimony to Congress regarding issues I found with IT management and recommendations for its improvement. I hope those efforts were, at least in some small way, helpful to Congress in shaping the FITARA legislation.

***Reflections on FITARA and the Scorecard***

FITARA has had a significant positive impact on agencies. 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 President Obama's, President Trump's, and now President Biden's Administration have handled the implementation of FITARA.

This spirit of bi-partisanship started with the drafting of FITARA, with the legislation being co-sponsored by Chairman Issa and, at the time, Ranking Member Connolly. And over the past six years, we have continued to see consistent oversight with the development and evolution of the FITARA Scorecard. Representatives Hurd, Meadows, and Kelly all have played leadership roles during this time. And today, Chairman Connolly and Ranking Member Hice continue to provide bi-partisan leadership on FITARA—it is heartening to see this level of dedication from Congress to help ensure better use of IT in government agencies.

In reflecting on the impact of FITARA and related oversight, the improvement in grades on the FITARA Scorecard over time tells part of the story. But, in addition, we have seen tangible improvements in federal IT, including:

- 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
- Improved CIO authorities with more CIOs reporting to the head or deputy head of the agency, and with CIOs having greater insight into and oversight of agency IT spending to foster costs savings.

Certainly, credit goes to the agency CIOs and their staff for the excellent work they do every day. But I reiterate that the significant difference from past efforts is consistent and sustained Congressional oversight.

### ***Current State of Federal IT***

Yet, even with the support of FITARA and the scorecard, much work remains in federal IT to reach a state of “best practice.” If there were unlimited funds to invest in IT, the federal government would still struggle because many of our agency IT organizations do not have the management maturity and skills to deliver large-scale IT modernization effectively. 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 the latest report on its High-Risk List, published in March 2021, GAO updated this particular high-risk item. While GAO gives OMB credit for demonstrating leadership commitment to address weaknesses in the management of IT acquisitions and operations, the report states that the government has only partially met requirements in the criteria for capacity, monitoring, action plan, and demonstrated progress elements of this high-risk item. And the ratings for all five criteria did not improve since the issuance of the 2019 report.

Of particular concern outlined in the report is that 21 of the 24 major federal agencies still had not implemented GAO's 2018 recommendations to modify their practices to fully address their CIO's role consistent with federal laws and OMB's FITARA guidance. Progress in establishing key IT workforce planning processes was also lacking—none of the recommendations GAO made to five agencies in a November 2016 report have been implemented. In terms of plans to modernize critical IT legacy systems, in 2019, GAO identified ten critical legacy systems that needed modernization. Of the ten agencies responsible for those legacy systems, seven agencies had documented plans for modernizing the systems. However, most lacked the key elements identified in best practices (milestones, a description of the work necessary to complete the modernization, and a plan for the disposition of the legacy system). The remaining three agencies did not have documented modernization plans. GAO made eight recommendations to eight agencies to address these weaknesses, but as of December 2020, the agencies had implemented none of the recommendations.

### ***Recommendations to Evolve the FITARA Scorecard***

Given the existing challenges in Federal IT, active, bi-partisan Congressional oversight is vital to continued progress. As described above, the FITARA Scorecard has been effective in helping drive successes in areas to include data center consolidation, software licensing, and the use of incremental delivery methods. Now is the time to substantively evolve the scorecard to address the core IT modernization challenges agencies face, as highlighted by GAO's audit work. The four recommendations presented below would have the most significant near-term impact on improving federal IT and, in particular, agencies' abilities to drive successful IT modernization.

**Add an "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 Planning, this measure would require an IG to annually audit an agency’s practices.

**Evolve 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 their IT budgets. On a positive note, the federal government has adopted the Technology Business Management (TBM) taxonomy, an industry standard for categorizing IT costs, enabling agencies to capture IT cost detail and determine what it costs to deliver their IT services. With such information, agencies can benchmark themselves in providing commodity IT services, such as standard desktop applications, collaboration tools (including 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 into how they stack up, with benchmarks from other similar-sized agencies and private-sector corporations.

Measuring this category could be relatively straightforward, with an agency receiving an F if there is no use of TBM, a D if an agency partially implements the TBM taxonomy, a C if an agency

fully implements the TBM taxonomy, a B if the agency is using TBM to benchmark basic IT commodity services, and an A if the agency is using TBM to benchmark complex IT services.

**Evolve the “Cybersecurity” Category** – It was appropriate a cybersecurity category was added to the scorecard, as cybersecurity is such an essential part of a CIO’s set of 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.

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 adopting and implementing a zero-trust architecture, having holistic visibility across one’s IT infrastructure, implementing secure computing guidelines in cloud computing environments, and focusing on protecting high-value data and system assets. Further, the EO addresses the need for the federal government to address supply chain issues related to cybersecurity, particularly software supply chain issues.

With the leadership of GAO and the support of DHS’s Cybersecurity & Infrastructure Agency (CISA), the steps outlined in the EO can serve as a means to derive a comprehensive set of measures that can more accurately assess an agency’s cybersecurity posture. And while it is desirable to use publicly-available data, Congress and GAO might consider using some non-public measures in this category, given they would provide a more accurate grade of an agency’s cybersecurity posture.

### ***Recommended Next Steps***

Certainly, any significant change to the FITARA Scorecard requires more in-depth analysis to determine the specific elements that would make up the measure for a category, and what additional data would be necessary for agencies to report to OMB and GAO. If Congress agreed to evolve the scorecard to the degree I am recommending, it would probably take two years to make all of the changes to the scorecard. However, the changes could be phased in over that period, so that every six months the scorecard would evolve.

The scorecard is a tool to support Congressional oversight. As such, it is Congress’ decision regarding the categories to include in the scorecard and the measures that constitute each category. Yet, given there is a bi-partisan agreement for the need to continue improving IT management in our government and the value of the scorecard, Congress should convene an advisory group that would develop recommendations to evolve the FITARA Scorecard. GAO should head this advisory group, but it should include representatives from the Federal CIO Council, the Office of the Federal CIO (within OMB), and the private sector (to ensure consideration of industry best practices). The American Council for Technology – Industry Advisory Council (ACT-IAC), a

unique, government and industry non-profit organization whose mission is to support government through the use of technology, could obtain the private sector input. ACT-IAC has already played a role in FITARA, providing support to OMB as they developed their guidance to agencies for FITARA implementation. Such an advisory group would gather recommendations from those testifying today and other interested parties. Over a three-to-six month period, the advisory group could provide Congress a set of proposed changes to the scorecard, proposed phasing for the changes, and a plan for implementing the changes in agency data collection necessary to enable Congress and GAO to grade each category properly.

The passage of FITARA, together with Congressional oversight most visibly demonstrated through the semi-annual publication of the FITARA Scorecard, has had a very positive impact on Federal IT. Yet it is also the case most agencies are still far from using best practices for IT management and have significant modernization challenges. Given the scorecard works, it should evolve to support and drive agencies to adopt IT management best practices more rapidly and move aggressively to modernize agency processes and systems.

Thank you for the opportunity to testify today.