Testimony of David Powner
Before the Subcommittee on Government Operations
of the
House Committee on Oversight and Reform
August 3, 2020

Chairman Connolly, Ranking Member Hice, and distinguished Members of the Subcommittee on Government Operations, thank you for the opportunity to testify before you on the Federal Information Technology Acquisition Reform Act (FITARA) scorecard and how it can evolve to continue to help federal agencies modernize and improve their security. For the past two years I have worked at MITRE, a 501(c)(3) not-for-profit corporation. We are chartered to operate in the public interest, which includes operating federally funded research and development centers, or FFRDCs, on behalf of federal agency sponsors. We currently operate seven FFRDCs. Our Center for Enterprise Modernization was established in 1998 by the Department of Treasury and we have been proud to support many modernization efforts under that FFRDC, which is now jointly sponsored by the Department of Veterans Affairs (VA) and the Social Security Administration (SSA). The other primary sponsors for which MITRE operates FFRDCs include the Department of Defense; the Centers for Medicare and Medicaid Services at the Department of Health and Human Services; the National Institute of Standards and Technology; the Federal Aviation Administration; the Department of Homeland Security; and lastly, the U.S. court system, the only FFRDC sponsored by an agency outside of the Executive Branch.

Prior to joining MITRE, I served as the Director of IT issues at the Government Accountability Office (GAO), leading their information technology audits related to over $80 billion in information technology spending across the federal government. During that time, I had the opportunity to work closely with this Committee drafting FITARA, helping with the creation of the FITARA scorecard, and assisting in your oversight efforts. I testified at the first six FITARA scorecard hearings.

Observations on FITARA's Impact

FITARA pumped new energy into the federal IT community with its focus on reinforcing CIO authorities, optimizing data centers (which were severely underutilized), and strengthening acquisition management. The results we've seen from this 2014 law are significant:

- Billions of taxpayer dollars have been saved consolidating data centers and reducing duplicative business systems and licenses,
- Acquisitions are now tackled in more manageable increments which has helped deliver services to citizens in a more timely manner and within cost estimates, and
- CIOs authorities and relationships with CFOs have been strengthened, resulting in taxpayer dollars being spent more efficiently.

So why did FITARA work? There have been plenty of prior IT laws that have fallen far short of expectations. It worked because of the actions of Congress, OMB, and agency CIOs over the past five-plus years. Let's explore these, looking at what we can learn and how we can emulate these actions with future legislation, oversight, and management.

Congress – This Committee, with support from GAO, has performed thorough and consistent oversight on agencies' implementation of the law using the FITARA scorecard to measure progress. Never have we seen such follow-through on an IT law. Chairman Connolly, who co-created FITARA with then-Chairman Issa, has been at every hearing and has worked behind the scenes constructively pushing agencies to improve. Chairman Connolly has also had plenty of bipartisan support on this effort - Representatives Kelly, Hurd, Meadows and now Ranking Member Hice have been key partners. This has been a model of bipartisan oversight.

OMB – Federal CIOs have played a key role. OMB issued FITARA implementation guidance soon after the law was passed, and Federal CIOs including Tony Scott and Suzette Kent have supported agency CIOs as they strengthened their management of IT acquisitions and operations. In response to this leadership, agency CIOs have stepped up across the federal government demonstrating leadership and delivering results. In addition, OMB's budget support for key FITARA tenets helped provide the resources necessary to act on these priorities.

Evolution of the Scorecard

The first scorecard in November 2015 had four categories that were graded, all of which were major sections of the FITARA legislation – (1) incremental delivery, (2) IT dashboard transparency and risk management, (3) portfolio management, and (4) data center optimization. Over time, three additional areas were added to the scorecard that are each associated with IT legislation. These three are:

- Software licensing – a requirement in the Making Electronic Government Accountable By Yielding Tangible Efficiencies (MEGABYTE) Act of 2016.
- Working capital funds – a requirement in the Modernizing Government Technology (MGT) Act of 2018.
- Cybersecurity – a requirement in the Federal Information Security Management Act of 2002 (and amended in 2014).

In addition, the scorecard reinforced the importance of establishing a direct reporting relationship between agency CIOs and deputy secretaries.

Considerations for Future Scorecards

Ten scorecards later, we see significant progress in the original four areas graded, as well as in software licensing. The working capital funds and cybersecurity categories still, in my opinion, show room for improvement. We need to build off successes and take on additional, and at times, more challenging areas confronting agency CIOs. This might include eliminating or retiring certain categories where great progress has already been realized. This doesn't mean they aren't important, it just means that they've achieved a level of maturity to be sustainable. This would also help to keep the scorecard focused on those areas in which further improvement or sustained performance is needed. Here are five recommendations to consider for future scorecards.

1. **Enhance the cybersecurity category**. Cybersecurity should always be front and center on CIO and CISO's radars. The current grading uses OMB's ten cybersecurity Cross Agency Priority (CAP) goal metrics that are associated with authorization, personal

access and intrusion detection. Federal CISOs often have a consistent yet more robust set of cyber metrics that they manage to. There is an opportunity for OMB to improve these metrics with input from DHS in its cyber leadership role, CISOs and industry. In addition, the current Inspector General component of the current scorecard becomes dated rather quickly and may not provide an accurate characterization of an agencies' security posture.

2. **Add an infrastructure category**. This category could include data centers where opportunities for efficiencies remain, but more importantly should incorporate agency progress leveraging GSA's 15-year, $50 billion Enterprise Infrastructure Solutions (EIS) contract vehicle. This contract vehicle allows for a more modern and secure telecommunications infrastructure.
3. **Add an IT budgeting/funding category**. This category should continue to include 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 modest increases if we are to modernize to the extent needed and turn the corner on 80 percent-plus spend on legacy operations. Agency IT budgets need to better reflect their IT needs.
4. **Add an IT workforce category**. IT leaders and professionals with expertise and experience in cybersecurity and other technical disciplines need to be increased and retained throughout the federal government. Having transparency on workforce gaps would be helpful because it is a critical success factor, and some agencies may need to make additional investments to attract and retain this talent in a very competitive environment. As an example, although not directly tied to this scorecard discussion, Congress should look at using more critical pay authorities for CIOs, as well as examining five-year appointment terms for CIOs to address the short tenure problem and its impact on mission modernization.
5. **Add a mission modernization category**. Addressing the nation's most critical legacy systems remains a major challenge. They are fraught with unsupported hardware and

> software and oftentimes are operating with known security vulnerabilities. We should highlight these mission modernization priority areas on the IT Dashboard and have OMB play a greater role in securing funding and tracking progress. Ultimately, this category should track vulnerable legacy systems retirements and the customer/citizen experience with the new systems. These legacy systems force agencies to operate business processes the same way they have for decades. So, this is a perfect opportunity to modernize agencies' business processes along with the technology to enhance services to citizens.

With the bipartisan leadership of Chairman Connolly and many others, the FITARA Scorecard has been a great driver of progress for federal IT modernization, but we can and should do more. These recommendations can serve as a starting point for an ongoing process of continuous evaluation and improvement.

On behalf of the entire MITRE team, I greatly appreciate the opportunity to come before you again today and I look forward to your questions.