Testimony of David Powner
Before the Subcommittee on Government Operations
of the
House Committee on Oversight and Reform
January 20, 2022

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 operations and security. For the past three 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 six FFRDCs. Our Center for Government Effectiveness and 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 which operates the National Cyber Center of Excellence; the Federal Aviation Administration; and the Department of Homeland Security.

Currently, I lead MITRE's Center for Data-Driven Policy, where we connect our deep expertise on topics like engineering, acquisition, and cybersecurity to policymakers in both the legislative and executive branches. For instance, MITRE's expertise has recently been solicited on cybersecurity and customer experience legislation and executive orders.

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, then again in August 2020 on scorecard 10.0. During this latest hearing, I recommended scorecard modifications and my testimony today builds on those recommendations.

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 software licenses, and
- Acquisitions are now tackled in more manageable increments, which has helped deliver services to citizens in a more timely manner and within cost estimates.

So why did FITARA work when plenty of other IT laws have fallen far short of expectations? It worked because of the actions of Congress, OMB, and agency CIOs over the past seven 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, using data and metrics to drive outcomes. 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 – Ranking Member Hice and Representatives Kelly, Hurd, and Meadows have been key partners. This has been a model of bipartisan oversight.

OMB and Agency CIOs – Federal CIOs have played a key role. OMB issued FITARA implementation guidance soon after the law was passed, and Federal CIOs including Tony Scott, Suzette Kent, and now Clare Martorana have supported agency CIOs as they strengthened their management of IT acquisitions and operations. In addition, OMB's budget support for key

FITARA requirements helped provide the resources necessary to act on these priorities. In response to this leadership, agency leaders and CIOs have stepped up across the federal government working collaboratively and delivering results.

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, four additional areas were added to the scorecard that are each associated with IT legislation or a significant Administration priority. These four are:

- Software licensing – a requirement in the Making Electronic Government Accountable By Yielding Tangible Efficiencies (MEGABYTE) Act of 2016. (included initially on scorecard #4, June 2017).
- Working capital funds – a requirement in the Modernizing Government Technology (MGT) Act of 2018. (included initially on scorecard #6, May 2018).
- Cybersecurity – a requirement in the Federal Information Security Management Act of 2002 (and amended in 2014). (included initially on scorecard #6, May 2018).
- GSA's Enterprise Infrastructure Solutions (EIS) program – a 15-year, $50 billion contract that provides federal agencies with mission-critical telecommunications infrastructure and IT services to support their IT and security modernization efforts. (included initially on scorecard #11, December 2020).

One area has been removed from the scorecard, software licensing, in December 2020, with the issuance of the 11th scorecard, after all agencies received an "A" in this category. When this area was first graded in June 2017, there were 2 "A's", 1 "C", and 21 "F's".

Considerations for Future Scorecards

Consistent with my testimony in August 2020 on scorecard 10.0, we are recommending significant updates to the scorecard. Additional areas should be retired where significant

progress has been realized, some areas need to remain and be enhanced, like cybersecurity, and a completely new area on the IT and cyber workforce should be added.

Specifically, three additional areas should be retired – incremental, portfoliostat, and data centers – along with software licensing. This doesn't mean they are not important; it just means that they have achieved a level of maturity that's sustainable. The remaining four areas should be incorporated within the suggested five categories for future scorecards. We need to build off successes and take on current challenges confronting agency CIOs. 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 more robust set of cyber metrics that they manage to. There is an opportunity for OMB to improve these metrics with input from the National Cyber Director, the Federal CISO, DHS in its cyber leadership role, CISOs, and industry. In addition, the current Federal Information Security Management Act (FISMA) Inspector General component of the current scorecard becomes dated rather quickly and does not provide an accurate characterization of an agency's security posture. Specifically, the Inspector General portion of the category should be dropped and metrics consistent with Executive Order 14028 and zero trust tenets (e.g., multi-factor authentication) should be used to grade agencies' cybersecurity posture. Also, agencies' supply chain risk management (SCRM) maturity should also be considered as part of this grading. GAO has a comprehensive governmentwide report on SCRM that could be the basis for this grading. SCRM could also be its own separate category, given the risks here and the emphasis the Committee wants to place on it.

2. **Add an infrastructure category**. This category should include the recently added GSA 15-year, $50 billion Enterprise Infrastructure Solutions (EIS) contract vehicle, and should also include a cloud migration metric. This will advance the data center optimization initiative that, to date, has resulted in significant progress on cloud adoption across the federal enterprise. A cloud migration metric could even be expanded over time to be much broader than just having an infrastructure focus and could be focused on mission modernization and improved cybersecurity. Metrics could include the number of legacy application that have been migrated from on-premises data centers to the cloud, and how many new applications or services are utilizing cloud capabilities. Because of this, cloud migration, similar to SCRM, could also be a separate category on the scorecard.
3. **Add an IT budgeting/funding category**. 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.
4. **Add a mission modernization category and track this on the IT Dashboard**. 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 agencies' top 3 mission modernization acquisitions on the IT Dashboard and have OMB play a greater role in securing funding and tracking progress. There are many potential ways to manage these unsupported and insecure legacy applications. For instance, 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). Another option could be reporting, consistent with DHS CISA's guidance, software that contains critical security vulnerabilities. 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.

5. **Add an IT workforce category**. IT leaders and professionals with expertise and experience in cybersecurity and other technical disciplines need to be hired 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 and CISOs, as well as examining five-year appointment terms to address the short tenure problem and its impact on mission modernization.

In summary, we are proposing five future areas to the scorecard – cybersecurity, legacy modernization, workforce, infrastructure, and budgeting – with the option of also adding supply chain risk management and cloud adoption. With the bipartisan leadership of Chairman Connolly and Ranking Member Hice, 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, we look forward to continuing to help our sponsors secure and modernize their critical operations. I greatly appreciate the opportunity to come before you again today and I look forward to your questions.