Testimony of David Powner
Before the Subcommittee on Cybersecurity, Information Technology, and Government Innovation
of the
House Committee on Oversight and Accountability
May 10, 2023

Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, thank you for the opportunity to testify before you on Federal Legacy Information Technology (IT). For the past four 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 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), Department of Commerce 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 Cybersecurity Center of Excellence; the Federal Aviation Administration; and the Department of Homeland Security.

Currently, I lead MITRE's Center for Data-Driven Policy. We draw upon our deep expertise on topics like engineering, acquisition, and cybersecurity to bring non-partisan, evidence-based insights to policymakers in both the legislative and executive branches. For instance, MITRE's expertise has recently been solicited on cybersecurity legislation and executive branch policies ranging from artificial intelligence to biosecurity.

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 $100 billion in information technology spending across the federal government. During that time, I had the opportunity to work closely with this Committee drafting the Federal Information Technology Acquisition Reform Act (FITARA) and the Modernizing Government Technology (MGT) Act,

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 and in January 2022 on scorecard 13. At those hearings, I recommended scorecard modifications that included having a legacy modernization category.

My statement today is based on a March 2023 paper I co-authored with Nitin Naik, MITRE Technical Fellow, providing a call to action across several urgent priorities to address our legacy IT challenges, and recommendations for OMB, Congress, federal agencies, and industry.

The Call to Action is Loud and Clear

Significant numbers of critical federal information technology systems that provide vital support to agencies' missions are operating with known security vulnerabilities and unsupported hardware and software. These legacy systems support important missions like wartime readiness and the operation of dams and power plants. They also host sensitive taxpayer and student data. The Government Accountability Office (GAO) has reported on these systems since 2016, highlighting security risks, unmet mission needs, and the increased maintenance costs associated with outdated systems. Most recently, GAO reported that some legacy systems are more than 60 years old, with some operating software that is up to 15 versions out of date.[1] The recent Federal Aviation Administration's (FAA) systems outage that cancelled 1,300 flights and delayed more than 10,000 in a single day highlights both the criticality of these legacy systems and the impact that a single outage can have on our transportation network and on the daily lives of thousands of citizens.

Of the $100 billion the federal government spends annually on IT, roughly 80 percent goes toward operating and maintaining existing systems. Over the last 18 months, the calls for action from key stakeholders across Congress, agencies, technical experts, and industry, to address

[1] GAO, Information Technology: Federal Agencies Need to Address Legacy Systems, GAO-16-248 (May 25, 2016). GAO, Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems, GAO-19-471 (June 2019). Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements, GAO-23-104719 (January 2023).

this disproportionate spending and to phase out these archaic systems have been loud and clear:

- In late 2021, MITRE's Center for Data-Driven Policy published a paper that identified eight recommendations to Congress to update the Federal Information Security Modernization Act of 2014 to meet the advanced threats posed by China, Russia, ransomware gangs, and other nation-state and criminal actors. One recommendation was to identify and modernize complex legacy IT systems to reduce costs and vulnerability. We also highlighted a recent MITRE analysis that shows that systems using many programming languages have disproportionately higher maintenance costs and security vulnerabilities.
- In early 2022, we testified at the Federal Information Technology Acquisition and Reform Act (FITARA) 13 scorecard hearing on changes to make the scorecard more effective. One of our recommendations was to add a mission modernization category to the scorecard and track progress using the IT Dashboard**.** Specifically, we recommended that each agency track its top three mission modernization acquisitions on the IT Dashboard, and that OMB play a greater role in securing funding and tracking progress on acquisitions, legacy systems retirements, and improvements to the customer/citizen experience.
- Last year, Senator Maggie Hassan introduced the Legacy IT Reduction Act of 2022 (S. 3897) that required (1) agencies to develop an inventory of legacy IT systems, (2) a plan to modernize these systems, and (3) the Office of Management and Budget (OMB) to issue guidance on the bill's implementation.
- In July 2022, OMB and the Office of the National Cyber Director (ONCD) issued a memorandum highlighting cyber investment priorities for 2024 budget submissions. These priorities include zero trust implementation, securing our critical infrastructure, supply chain risk management, and IT modernization (including accelerated adoption and use of secure cloud infrastructure).
- In September 2022, the American Council for Technology-Industry Advisory Council (ACT-IAC) issued a report that I helped to author that contained a series of

recommendations for evolving the FITARA scorecard. One recommendation was to have an IT Modernization Planning and Delivery Category in which agencies would get a letter grade of "C" if they had a comprehensive modernization plan reflected in their budget submission. Agencies could achieve higher grades by delivering on key acquisitions and decommissioning legacy systems.

- Most recently, the White House issued its updated national cybersecurity strategy in March 2023, calling for OMB to develop a plan to accelerate IT modernization at agencies, prioritizing the elimination of legacy systems.

Obstacles to Progress

Despite all the attention to this challenge, many agencies lack comprehensive IT modernization plans. When they do exist, not enough is done to implement them. Reasons for the lack of progress, include:

- The complexity of upgrading older versions of software that are constantly changing to address legislative changes and associated business rules over decades, along with the increasing challenge of finding programmers proficient in these older programming languages;
- The reluctance to accept the risks associated with transferring backend mission critical processing on large mainframe hardware to current big data servers and cloud technologies while trying to keep citizen-centric services available around the clock;
- A short-term focus that is driven by annual budgets and quick fixes, and short tenures of our IT leaders (average federal CIO tenure is under 2 years); and
- The lack of executive branch policies and legislation calling for focused attention to these systems, multi-year budgets to support modernization, and accountability mechanisms to ensure new systems are put in place and older ones retired.

Ten Recommendations for OMB, Congress, Agencies, and Industry

Without a modern 21st century digital government, federal agencies cannot fully harness the power of technology to advance their missions and improve citizens' experience with the

federal government. We offer these recommendations to OMB, Congress, federal agencies, and industry—who all play a critical role in prioritizing and modernizing our mission critical systems.

OMB

1. OMB should provide guidance to agencies that requires them to develop a prioritized inventory of legacy systems and an IT modernization plan. This guidance should articulate evaluation criteria to prioritize systems most in need of replacement. Criteria should include systems no longer supported, systems with known cybersecurity vulnerabilities, cost savings, and significant improvements to mission. The modernization plan should sequence acquisitions based on these criteria, and should address items such as network infrastructure, cloud migration, and cybersecurity. The plan should also include a decommissioning schedule that has clear milestones for retiring legacy systems. OMB should strongly consider requiring independent evaluations of agencies' inventory assessments and associated modernization plans.
2. OMB needs to ensure that there is a reporting/transparency mechanism to monitor progress and ensure accountability. This mechanism should leverage the IT Dashboard and clearly show progress, in terms of acquisitions and retirements, against the modernization plan.
3. OMB should establish a program under the federal CIO similar to the United States Digital Service effort that includes a public-private partnership with key technology industry providers, so that agencies which are not making enough progress on converting their legacy applications can seek assistance. This program should provide expertise on converting/re-engineering/redesigning older systems based on technologies from the previous century to newer current century technologies in a smooth non-disruptive manner that supports continuity of operations for federal agencies' mission critical processing and data management capabilities.

Congress

4. Congress should enact legislation similar to the Legacy IT Reduction Act of 2022 to ensure that our approach to legacy modernization spans subsequent Administrations

and requires modern acquisition practices, notably Agile techniques and a DevSecOps delivery pipeline to ensure continuous integration and delivery to accelerate acquisition.

5. Congress should implement the FITARA scorecard recommendations called for in the ACT-IAC report, including the IT Modernization Planning and Delivery Category.

Agencies

6. Agencies need to implement OMB guidance and new legislation by developing prioritized inventories, modernization plans, and budgets to support these plans.
7. Agencies need to report progress against those plans on the IT Dashboard. This would include updates to inventories and plans, acquisitions delivered, cloud offerings deployed, and legacy systems that are decommissioned.
8. Agencies should partner with the industry, national labs, or FFRDCs to find ways to apply artificial intelligence, machine learning, robotic process automation, and big data processing to extract business rules and data processing logic from legacy IT platforms like mainframes with assembly or COBOL languages. This logic has been developed over the last few decades in response to legislation, policy, fraud patterns, and data quality issues. This approach is similar to what DARPA, NSF, and other R&D agencies have used to identify creative ways to solve existing technology obstacles.

Industry

9. Industry needs to be a collaborative partner working closely with federal agencies on their IT modernization plans and execution against those plans.
10. Industry should bring innovative approaches to create new ways of transitioning systems and software created during the last century to the current industry prominent hardware and software platforms.

In summary, this legacy crisis needs a strong Congressional push to ensure that the right plans, actions, and budgets are in place. This subcommittee's leadership both from a legislative lens and oversight actions are critical to securing and advancing our nation's mission critical operations.

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.