TEN RECOMMENDATIONS TO MODERNIZE ARCHAIC AND INSECURE LEGACY APPLICATIONS

10 Recommendations to Address the Federal Legacy Systems Challenge

OMB

1. Guidance on legacy systems inventories and IT modernization plans
2. Transparency mechanisms to ensure progress and accountability
3. Establish a centralized public-private partnership where agencies can seek assistance

CONGRESS

4. Legacy IT reduction legislation
5. Enhancements to the FITARA scorecard

AGENCIES

6. Develop inventories, modernization plans, and supporting budgets
7. Report progress on acquisitions and retirements
8. Partner with industry, labs, and FFRDCs to apply artificial intelligence, machine learning, and robotic process automation to assist in the conversion effort

INDUSTRY

9. Be a collaborative partner to drive delivery and smooth non-disruptive transition of operations
10. Bring innovative approaches to transition efforts

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since 2016, highlighting security risks, unmet mission needs, and the increased maintenance costs associated with outdated systems.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reported that some legacy systems are more than 60 years old, with some operating software that is up to 15 versions out of date.[1] The recent Federal Aviation Administration's systems outage that canceled 1,300 flights and delayed more than 10,000 in a single day highlights both the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.

The Call to Action Is Loud and Clear

Of $100 billion the federal government spends annually on information technology (IT), 80 percent goes toward operating and maintaining existing systems. Over the past 18 months, the calls for action to address this disproportionate spending and to phase out these archaic systems have been loud and clear:

What Did We Learn?

- 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) 13.0 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 the Office of Management and Budget (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 develop an inventory of legacy IT systems, (2) agencies create a plan to modernize these systems, and (3) OMB issue guidance on the bill's implementation.
- In July 2022, OMB and the Office of the National Cyber Director 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 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. Senior OMB officials requested more content on four planning documents cited in the report (IT Modernization Plan, Cloud Adoption Plan, Zero Trust Architecture Plan, and IT Workforce Strategic Plan). Outlines for these plans were issued in February 2023.
- Most recently, the White House issued the 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 and the Need for Comprehensive Strategies

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 Chief Information Officer (CIO) tenure is under two years); and
- The lack of executive branch policies and legislation calling for focused attention to these systems, multiyear budgets to support modernization, and accountability mechanisms to ensure new systems are put in place and older ones retired.

10 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—which all play a critical role in prioritizing and modernizing our mission critical systems.

OMB

1. OMB should provide guidance to agencies that requires they 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 this 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 that 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 the federal government's approach to legacy modernization spans subsequent administrations.
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 industry, national labs, or federally funded research and development centers (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 past few decades in response to legislation, policy, fraud patterns, and data quality issues. This approach is similar to what the Defense Advanced Research Projects Agency (DARPA), the National Science Foundation (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 past century to the current industry-prominent hardware and software platforms.

About the Authors

Nitin Naik is a technical fellow at MITRE. He is an IT leader with extensive experience designing, operating, and managing IT systems and organizations to address business problems and deliver services in educational, financial, social science, and R&D enterprises.

Dave Powner is the executive director of MITRE's Center for Data-Driven Policy. He previously led GAO's IT management reviews, working closely with Congress, OMB, and federal chief information officers on IT reform efforts, including the Modernizing Government Technology Act, FITARA, and the FITARA scorecard.

For more information about this paper or the Center for Data-Driven Policy, contact policy@mitre.org.

Endnotes

[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). GAO, Information Technology: IRS Needs to Complete Modernization Plans and Fully Address Cloud Computing Requirements, GAO-23-104719 (January 2023).

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED. PUBLIC RELEASE CASE NUMBER PR_ 23-1079