PRESIDENTIAL TRANSITION: PRIORITY TOPIC MEMO
SEPTEMBER 2024

MITRE | Center for Data-Driven Policy

RECOMMENDATIONS TO MODERNIZE ARCHAIC AND INSECURE LEGACY SYSTEMS

Significant numbers of critical federal information technology (IT) 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since 2016, highlighting the security risks, unmet mission needs, and increased maintenance costs associated with outdated systems.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reported that some legacy systems are more than 60 years old, with some operating software that is up to 15 versions out of date.[1] In addition, many of the systems do not support multi-factor authentication, and as a result they are unable to support the desired zero trust approach called for in federal policy. Last year, the Federal Aviation Administration's systems outage that canceled 1,300 flights and delayed more than 10,000 in a single day highlighted 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 Case for Action

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

- In 2022, 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) Office of Management and Budget (OMB) issue guidance on the bill's implementation.
  In 2023, the Senate reintroduced this legislation (S. 2032).

- 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).

3 Recommendations to OMB for Modernizing Legacy IT

Provide guidance to develop IT modernization plans and budgets

Use the IT Dashboard to monitor progress

Utilize public-private partnerships to address modernization efforts

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.

- In September 2022, the American Council for Technology-Industry Advisory Council (ACT-IAC) issued a report containing a series of recommendations for evolving the Federal IT Acquisition Reform Act (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, in March 2023 the White House issued the National Cybersecurity Strategy, calling for OMB to develop a plan to accelerate IT modernization at agencies and prioritizing the elimination of legacy systems. Subsequent implementation plans in July 2023 and May 2024 reiterate that OMB has this task.

Obstacles to Progress and the Need for Comprehensive Strategies

Despite all the attention to this challenge, many agencies lack comprehensive IT modernization plans. When plans 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 and knowledge of the operational rules of the software
- 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 the short tenures of government IT leaders (e.g., the average federal Chief Information Officer [CIO] tenure is shorter than two years)
- 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

Data-Driven Recommendations for OMB and Federal Agencies

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 the incoming administration:

1. OMB, within the first 100 days, should provide guidance that requires agencies to develop a prioritized inventory of legacy systems, an IT modernization plan, and supporting budgets. 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. The guidance and supporting budgets need to include use of the Technology Modernization Fund and working capital funds called for in the Modernizing Government Technology Act of 2017.

2. OMB, within 180 days, needs to make sure a reporting/transparency mechanism is in place to monitor progress and ensure accountability. This mechanism should leverage the existing IT Dashboard and clearly show progress, in terms of acquisitions and retirements, against the modernization plan.

3. OMB, within 180 days, 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, or 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.

4. Agencies need to implement OMB guidance and new legislation by developing prioritized inventories, modernization plans, and budgets to support these plans. Agencies also 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 decommissioned.

5. 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, National Science Foundation, and other R&D agencies have used to identify creative ways to solve existing technology obstacles.

Recommendations for Congress and Industry

We offer these recommendations for Congress and industry because they also play a critical role in prioritizing and modernizing our mission-critical systems:

1. Enact legislation similar to the Legacy IT Reduction Act of 2023 to ensure that the federal government's approach to legacy modernization spans subsequent administrations.
2. Implement the FITARA scorecard recommendations called for in ACT-IAC's report, including the IT Modernization Planning and Delivery Category.
3. Enlist industry to be a collaborative partner working closely with federal agencies on their IT modernization plans and execution against those plans. Industry could bring new ways of transitioning systems and software created during the past century to the current industry-prominent hardware and software platforms.

MITRE Resources and Support

MITRE brings decades of experience addressing agencies' modernization needs. Our multidisciplinary IT modernization expertise has advanced both civilian and defense federal operations. Since 2021, we have called for more focused attention and policy actions to address our nation's legacy modernization challenges. Highlights include:

- M. Peters, et al. Eight Recommendations for Congress to Improve Federal Cybersecurity. MITRE. November 2021. https://www.mitre.org/sites/default/files/2021-11/pr-21-3403-eight-recommendations-for-congress-to-improve-federal-cybersecurity.pdf. One recommendation was to identify and modernize complex legacy IT systems to reduce costs and vulnerability.

- Testimony of Dave Powner Before the Subcommittee on Government Operations of the Committee on Oversight and Reform. January 20, 2022. Title of Hearing: FITARA 13.0. https://docs.house.gov/meetings/GO/GO24/20220120/114337/HHRG-117-GO24-Wstate-PownerD-20220120.pdf. 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.

- N. Naik, et al. Ten Recommendations to Modernize Archaic and Insecure Legacy Applications. MITRE. March 2023. https://www.mitre.org/sites/default/files/2023-03/PR-23-1079-Ten-Recommendations-to-Modernize-Legacy_Modernization.pdf. One of our recommendations was that agencies should partner with industry and FFRDCs to apply artificial intelligence and machine learning to assist in legacy migration efforts.

- Testimony of Dave Powner Before the Subcommittee on Cybersecurity, Information Technology and Government Innovation of the House Committee on Oversight and Accountability. May 10, 2023. Title of Hearing: Risky Business: Costly Inaction on Federal Legacy IT. https://oversight.house.gov/wp-content/uploads/2023/05/Powner-Legacy-IT-House-Oversight-Testimony.pdf. This testimony summarized Congressional recommendations we made in our March 2023 report.

- Under MITRE's Independent R&D program, we are currently researching the viability of using large language models to understand code and facilitate modernization. This research is being conducted in an emulated cloud environment with mission-critical applications from federal agencies.

About the Center for Data-Driven Policy

The Center for Data-Driven Policy, bolstered by the extensive expertise of MITRE's approximately 10,000 employees, provides impartial, evidence-based, and nonpartisan insights to inform government policy decisions. MITRE, which operates several federally funded research and development centers, is prohibited from lobbying. Furthermore, we do not develop products, have no owners or shareholders, and do not compete with industry. This unique position, combined with MITRE's unwavering commitment to scientific integrity and to work in the public interest, empowers the Center to conduct thorough policy analyses free from political or commercial pressures that could influence our decision-making process, technical findings, or policy recommendations. This ensures our approach and recommendations remain genuinely objective and data-driven.

Connect with us at policy@mitre.org.

Endnote

[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).