

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051

<https://oversight.house.gov>

Ranking Member Gerald E. Connolly

Subcommittee on Cybersecurity, Information Technology, and Government Innovation

Hearing on “Risky Business: Costly Inaction on Federal Legacy IT”

May 10, 2023

To best accomplish their public service missions, federal agencies need information technology (IT) systems that are efficient, effective, and secure. From facilitating veterans’ online access to health and pension benefits to processing millions of taxpayers’ vital IRS refunds, IT keeps our country running 24-hours a day, seven days a week. But as we know, not all IT systems are created equal. In fact, the Government Accountability Office (GAO) found that of the \$100 billion dedicated to information technology and cyber-related investments, 80% of those dollars are spent on technology operation and maintenance expenses alone, including legacy systems.

While age itself is not inherently an indication of poor performance, legacy systems—those that are written in outdated languages or are operating on unsupported hardware and software, leave our government vulnerable to security threats. It is vital, therefore, that we work together to identify and update the legacy systems that plague federal agencies.

During my tenure as Chairman of the Government Operations Subcommittee, I focused the gavel on IT modernization. Over the course of eight hearings in the 117th Congress alone, we established that achieving quality IT demands three components: cost effectiveness, prioritized customer experience, and a robust cyber infrastructure. While each of these factors may seem independently important, they are related and create the foundation for agency success.

That is why, I am immensely proud to have worked with my former Republican colleagues to establish the Technology Modernization Fund (TMF). We engineered the TMF to reimagine and transform the way federal agencies invest in modern, nimble technology and deliver services to families, businesses, and communities. We wrote the TMF with clear intent to provide a flexible funding stream outside of the traditional appropriations process. We sought to enable multi-year investments that catalyze sweeping, complex, and transformative IT projects. TMF-funded IT modernization projects lower agency operating costs over time and fortify cybersecurity. Agencies whose TMF investments yield cost savings could repay the fund within a designated timeframe, helping to establish a more self-sustaining IT modernization resource.

Last year, the White House announced it would designate \$100 million of the revolutionary \$1 billion infusion in the TMF that I fought for and secured within the American Rescue Plan, to improve federal agency customer experiences. The investments, if made wisely will reduce wait times for vital services, eliminate duplicative, time-consuming paperwork, and remove bureaucratic barriers that waste taxpayers’ time and federal agency resources. These efforts will rebuild public trust between society and their public institutions.

I am proud to note that out of the 39 projects that secured TMF investments across 24 agencies, GAO estimates that 25 have aspects of cybersecurity, with 11 projects primarily focusing on security issues. By upgrading

vulnerable systems, our federal government can better protect itself and the people it serves from data breaches, critical infrastructure hacks, and the leakage of national security information. **I hope to continue this Subcommittee’s bipartisan tradition and work with my colleagues on the other side of the aisle to reauthorize this program once GAO publishes its third and final statutorily-required report on the TMF, which is due this December.**

I also remain committed to using the FITARA Scorecard as a tool to modernize legacy IT. Over its past 15 iterations, this oversight effort has resulted in more than \$6.6 billion in cost savings and avoidances from 2012 to 2021 alone. The lion’s share of this success comes from the closure of unnecessary federal data centers and agencies’ migration of their IT capabilities to the cloud. The Scorecard also works hand in glove with the goals of the National Cybersecurity Strategy, including pushing for the elimination of legacy IT systems. The Strategy notes that legacy systems are often unable to implement zero-trust architecture, leaving agencies susceptible to sophisticated cyber threats.

As a result of these concerns, our Subcommittee recently updated the new cybersecurity metric on the FITARA Scorecard to include zero trust as a component of the score. This evolution of the Scorecard incentivizes agencies to modernize and stay in front of emerging cyberthreats. In addition, the Scorecard has also improved agencies’ IT investment and development strategies by addressing cost overruns, schedule slippages, and poor project management. We must improve how we track IT modernization planning and implementation. We know what happens when an agency doesn’t have a plan, doesn’t have timelines for project completion, and is not delivering on its modernization goals. In a recent GAO study I requested, GAO found the IT challenges at the IRS are substantial, due to planning and implementation deficiencies. Legacy IT costs are still unknown, modernization plans lack timelines for the disposition of legacy systems, nearly a quarter of the agency’s software inventory is legacy software, and the effort to replace the 60-year-old Individual Master File is on hold with no definitive end in sight. Lastly, the Scorecard emphasizes the need for agency IT working capital funds, separate appropriations accounts within an agency designated specifically for modernization and other essential IT investments that can be used outside of the rigid and sometimes unpredictable annual appropriations process.

Embracing modern and secure IT solutions is crucial for federal agencies to streamline operations, enhance cybersecurity, and fulfill their missions. I know that everyone on this dais is interested in and committed to ensuring we have a 21st century federal government for our constituents. I intend to continue our committee’s dogged oversight of federal agencies IT modernization effort to ensure we deliver on that commitment.

###

Contact: Nelly Decker, Communications Director, (202) 226-5181