RISKY BUSINESS: COSTLY INACTION ON FEDERAL LEGACY IT

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

MAY 10, 2023

Serial No. 118–28

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
52–162 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
JIMMY GOMEZ, California
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
BECCA BALINT, Vermont
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida

C O N T E N T S

WITNESSES

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

Documents are available at: docs.house.gov.

RISKY BUSINESS: COSTLY INACTION ON FEDERAL LEGACY IT

Wednesday, May 10, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:08 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Edwards, Langworthy, Burlison, Connolly, and Lynch.

Ms. MACE. All right. Good afternoon, you all. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will come to order. Welcome, everyone. Love those red glasses. Those are super cool.

Without objection, the Chair may declare a recess at any time, and I recognize myself for the purpose of making an opening statement.

Good afternoon, and welcome to this hearing of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation. An important role of this Subcommittee is ensuring Federal information technology is well managed, as you all are well aware. The Federal Government depends on IT systems for everything from national defense to homeland security to the administration of benefits programs.

In all, we spend upwards of $100 billion of tax dollars annually for Federal IT. Notably, 75 to 80 percent of this spend currently goes to operating and maintaining existing IT systems, and much of that infrastructure is aging and obsolete. It relies on a shrinking pool of workers versed in archaic programming languages like COBOL, which came into common use 60 years ago.

I, myself, learned COBOL when I was starting my career in the late 1990's, and even then we knew that it was a legacy IT system. In fact, I was in the financial services sector, working in COBOL, and if I see another line of COBOL code today I might vomit. I might throw up.

But at that time and now, computer coding provides a pathway for girls and women to advance into STEM fields, but gosh, I hope we can get beyond COBOL one day.

But today's aspiring young coders are not learning COBOL. That is why the government, whose aging IT workforce includes many more individuals over 60 than under 30—it is actually four times in terms of those that are looking at retirement in the next few years versus those that are coming in that are younger and more adept with computer engineering and programming.

A few years ago, GAO compiled a list of the 10 Federal IT systems most in need of overhaul due to their criticality and their obsolescence. One is a COBOL-based system used to process about 20 million Federal student financial aid applications annually. The system is older than the Department of Education, which opened its doors in 1980. That is kind of scary.

Another COBOL-based system on GAO's list is an IRS system containing taxpayer data, that went on-line in 1968, long before I was born, more than a half century ago. The IRS continues to keep taxpayer data on this system and other hugely outdated systems, despite pouring billions of dollars over the years into failed modernization efforts.

And I would be remiss if I did not add on, with the advent of AI, archaic legacy systems, archaic coding, consumer data, personal data, government data is all at a much higher risk today than it ever has been, and the way in which AI can be utilized to get after authentication, for example, puts us and our data, government and the private sector, those risks at an all-time high.

The Biden Administration is now set to hire 20,000 new auditors over two years as part of a massive $80 billion hike in IRS spending, but what the IRS needs most are modern computers and call centers to answer the phone.

What scares me is that Federal legacy computer systems are highly vulnerable to cyberattacks from malicious actors, including enemy nation states, and the danger is going to get a lot worse and fast. The rise of AI—oh, I looked at my notes; I already have AI and I already skipped ahead—will soon lead to increasingly sophisticated cyber assaults.

That is why it is more important than ever that data of millions of students and taxpayers do not live on half-century-old IT systems that are easily exploited by our enemies. So, we need to take and make progress on IT modernization by whatever means necessary and at our disposal.

A new funding vehicle, the Technology Modernization Fund, was created in 2017. It provided another tool for replacing legacy IT. But it has become clear that it is a tool that needs sharpening. So, I intend to introduce legislation soon that will do just that. I expect this hearing to help inform that bill. Congress must act to ensure taxpayer personally identifiable information and other sensitive data are not wide open for thieves or foreign actors to plunder.

The U.S. Chamber issued a statement. We have this beautiful letter today that we will enter into the record for today's hearing.

Ms. MACE. It says that a time when America is confronting inflation and budgetary stresses, Congress must look to find new and creative ways to solve fiscal challenges and improve services through government IT modernization, and I could not agree more.

This Subcommittee will continue to focus its oversight and legislative efforts on innovative solutions that actually move the needle

on the old problem of IT modernization, and that is what this legislation will do, that is what this hearing will do today, and it is my hope that if we do nothing else in this Committee, because I doubt that we will, that we can find some nonpartisan—I am not kidding—that we can find a way, both sides, to work on this issue. This is not a partisan issue. And I hope that you will work with us and our Committee in finding ways that we can sharpen the tools that we have going forward.

So, with that, I will yield to the Ranking Member of this Subcommittee, Mr. Gerry Connolly, of Virginia.

Mr. CONNOLLY. Thank you, Madam Chairwoman, and thank you for having this hearing and your commitment to this critical set of issues that challenge all of us.

To best accomplish their public service missions, Federal agencies need information technology systems that are efficient, effective, and secure. From facilitating veterans' on-line access to health and pension benefits to processing millions of taxpayers' vital IRS refunds, IT keeps our country running 24 hours, 7 days a week.

But as we know, not all IT systems are created equal, as you just pointed out, Madam Chair. In fact, the Government Accountability Office found that of the $100 billion or so dedicated to IT and cyber-related investments, as much as 80 percent of those dollars are spent on operation and maintenance expenses, including the legacy systems.

While age itself is not inherently an indication of poor performance, those that are written in outdated language, as you just indicated, like COBOL, or 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 need to be replaced.

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 robust cyber infrastructure. While each of these factors may seem independently important, they are related and create the foundation for agencies' success. That is why I am immensely proud to have worked my former Republican colleagues on this Subcommittee to establish the Technology Modernization Fund.

We engineered the TMF to re-imagine and transform the way Federal agencies invest in modern, nimble technology and to deliver services to families, businesses, and communities. We wrote the TMF with the clear intent to provide a flexible funding stream outside of the traditional appropriation process. We sought to enable multiyear investments that catalyze sweeping, complex, and transformative IT projects. TMF-funded IT modernization projects lower agency operating costs over time and fortify cybersecurity.

Last year, the White House announced it would designate $100 million of the revolutionary $1 billion infusion in the TMF to improve Federal agency customer experience. The investments, if made wisely, could 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 themselves and our public institutions.

I am proud to note that of the 39 projects that secured TMF investments across 24 agencies, GAO estimates that 25 have aspects of cybersecurity, with 11 projects primarily focused 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.

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 avoidance from 2012 to 2021, alone. The lion's share of this success comes from the closure of unnecessary data centers and agencies' migration to the cloud. The scorecard works hand-in-glove with the goals of the National Cybersecurity Strategy, including pushing for the elimination of legacy IT system.

As a result, our Subcommittee recently updated the new cybersecurity metric on the FITARA scorecard to include zero trust as a component of the score. This evolution incentivizes agencies to modernize and stay in front of emerging cyber threats. In addition, the scorecard has improved agencies' IT investment in 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 does not have a plan, does not have timelines for project completion, and is not delivering on its modernization goals.

In a recent GAO study that I requested, GAO found that IT challenges at the IRS, for example, 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 end in sight.

Last, 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 appropriation 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 that we have 21st century Federal Government for our constituents. I intend to continue our Committee's dogged oversight of Federal agencies' IT modernization effort to ensure that we live up to that commitment.

Again, I want to welcome our panelists. I have worked with all three, and I think they are great choices today, Madam Chairwoman, and I look forward to hearing their testimony. Thank you.

Ms. MACE. Thank you, Mr. Connolly. And today I am pleased to introduce our witnesses for today's hearing. Our first witness is

Mr. Kevin Walsh, Director of Information Technology at the U.S. Government Accountability Office, or GAO. The second witness is Ms. Suzette Kent, a global business transformation executive who has previously served as the Federal Chief Information Officer for the United States. And our third witness is Mr. David Powner, Director for the Strategic Engagement and Partnerships with the MITRE Corporation. We welcome everyone and we are pleased to have you here this afternoon.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise their right hands.

Do you solemnly swear or affirm that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

Mr. WALSH. I do.

Ms. KENT. I do.

Mr. POWNER. I do.

Ms. MACE. Let the record show that the witnesses all answered in the affirmative.

We appreciate all of you being here today and look forward to your testimony. Let me remind the witnesses that we have read your written statements and they will appear in full in the hearing record. Please limit your oral statements to five minutes. As a reminder, please press the button on the microphone in front of you so that it is on, and the Members up here can hear you.

When you begin to speak, the light in front of you will turn green. After four minutes the light will turn yellow, and when the red light comes on your five minutes has expired, and we would just ask that you please wrap up your comments.

I would like to recognize Mr. Walsh to please begin your opening statement.

STATEMENT OF KEVIN WALSH
DIRECTOR
INFORMATION TECHNOLOGY AND CYBERSECURITY
U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WALSH. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for inviting GAO to testify on this important issue.

I am sure you will not be surprised to hear that the government has a legacy IT problem. However, it is hard to know the true scope of the issue. According to the MGT Act, a legacy IT system is outdated or obsolete. To build on that, our Federal CIO has noted that not all old systems are legacy, and "old" does not necessarily mean bad, antiquated, risky, or in need of retirement. I agree. Replacing all of the old IT in the government would be a monstrous task and probably a waste of funds.

The Federal CIO is most concerned with legacy that is out of support, cannot be patched, has availability issues, or cannot meet user needs or policy goals—systems whose security cannot keep pace with adversaries. Again, I agree.

Those worrisome situations become more prevalent if we ignore our aging technology. As our systems get older they cost more to secure, more to maintain, do not always meet mission needs, and, in some cases, the only people who can update them are retired.

Some of these systems may persist because agencies are not required to identify and evaluate what should be kept. OMB drafted guidance in 2016 that would have required agencies to do exactly that. Regrettably, that guidance remains in draft form. To OMB's credit, their subsequent 2018 guidance on high-value assets could cover the most important legacy systems. However, the government cannot afford to ignore the rest of its IT.

In addition, the recently released National Cyber Strategy calls for Federal efforts to eliminate legacy systems that are costly to maintain and difficult to defend against sophisticated cyber threats. However, it will be hard for the government to eliminate legacy systems if we do not know what we have.

To do so, agencies would need an inventory of their IT systems, as called for in OMB's draft guidance. After that, agencies should identify their legacy systems, prioritize them to determine what we should keep, or modernize, replace, or retire. These decisions could be based on factors including how risky it will be, including risks to security and privacy, the criticality of the system, cost to modernize or maintain the current system as well as any potential cost savings, whether mission needs are being met, and if additional functionality or benefits could be gained.

To be clear, there will be instances where modernization may not make sense at this time. That is a good thing. We want agencies to be responsible stewards of taxpayer dollars. Having the newest toys and gadgets, like Batman, does not necessarily mean good governance or even good IT. There will also be modernizations that cost more money than they save. However, in those instances there should be other benefits that can be gained, such as increased cybersecurity, better functionality, or better performance.

These reviews of agencies' IT portfolios to identify legacy IT should also note be a one-time exercise, but they should be part of a core part of our portfolio management in the government.

Finally, as we modernize or replace our systems, we should make sure that the old systems get turned off.

This concludes my comments, and I look forward to your questions.

Ms. MACE. Thank you, Mr. Walsh.

And I now would like to recognize Ms. Kent for your five minutes.

STATEMENT OF SUZETTE KENT
CHIEF EXECUTIVE OFFICER
KENT ADVISORY SERVICES

Ms. KENT. Chairwoman Mace, Ranking Member Connolly, and distinguished Members of the Subcommittee, thank you for the opportunity to speak with you regarding Federal information technology.

This Committee has been unwavering in demonstrating bipartisan commitment to improving the mission outcomes of government through better uses of technology. Reminders of the dangers of archaic IT infrastructure are evident every day in both public and private sector—data stolen, travel disrupted, power grids compromised, people in businesses deprived of services, lives threatened, and our homeland security impugned.

And these dangers are like ticking time bombs, becoming more severe as the use of AI and the attacks on encrypted data become more sophisticated. And despite congressional and executive branch directives, despite creation of new funding vehicles, and the ever-present pressure of mission needs, some agencies have still struggled to make significant progress tackling that technical debt.

My comments today are going to draw my personal experiences of over 30 years in global technology and having served as the Federal CIO and working closely with IT teams to address these issues. But let us reflect very quickly on the current situation. The strategic plan and the annual budget process should be the primary lever, but it is not timely and budgets have been flat for the last decade.

The Technology Modernization Fund, it was created as a source for urgent needs and to provide a multiyear vehicle focusing on legacy IT transition, cybersecurity, and emerging technology, but it could use sharpening.

Working capital funds. This vehicle gives agencies flexibility, but not all agencies choose to establish a working capital fund. And we do have public-private partnerships and grants that are effective to explore new technology, but these are not scale options.

Although these tools have all yielded positive results, it is not at the pace of technology change or to scale that overcomes technical debt.

So, some areas for exploration for this Committee could be reestablishing priority, making legacy transition an agency priority, and updating how those outcomes are measured. Give agencies a specific directive, and update one of the various scoring mechanisms, ROI, FITARA, IT Dashboard, or potentially new measures to bring laser focus to agency progress, eliminating outdated technology.

As you heard from Mr. Walsh, there has long been ambiguity about defining legacy, but focus on cyber vulnerabilities and areas that hinder the mission goals and consider using the GAO reports of legacy systems with the most significant risks to aim these directives.

Enhance the planning processes by mandating comprehensive transformation plans with financial estimates and timelines. If directing agencies to produce a plan for migration for the most egregious applications, Congress could then validate those plans or incorporate it into agency strategic plans, supporting the funding base on those plans, and hold agencies accountable. In this way, Congress supports the actions from end to end, and this is very important because it is likely these efforts span multiple administrations, so bipartisan support is critical.

Modernizing the process for defining project value, expanding business case metrics to include things beyond cost savings, like risk reduction, value to mission, or improved resource availability, and very important, modernizing workforce.

Accelerate the Office of Personnel Management's commitment to expanding skills-based hiring for technology roles. Current technology use requires current skills, regardless if people lack traditional post-secondary academic degrees. Skills-based hiring should not be looked at as an exception, but as a real pathway forward

to rejuvenate the Federal workforce. Technology capabilities are available to do this, and they are proven.

Congress can accelerate overhaul of legacy systems by making it a clear priority, shining a light on what is wrong with the processes, focusing measurement funding on the problem, and using expanded pathways to bring in talent that can deliver this transition.

These are the areas that I would submit where Congress can be an accelerator for modernizing the technology that runs our government and serves the people of our Nation. Thank you.

Ms. MACE. Thank you, Ms. Kent.

And now Mr. Powner, you are recognized for your opening statement.

(Minority Witness)
STATEMENT OF DAVE POWNER
EXECUTIVE DIRECTOR
CENTER FOR DATA-DRIVEN POLICY
THE MITRE CORPORATION

Mr. POWNER. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to testify on Federal IT. I work for MITRE, a nonprofit corporation that operates in the public interest. Currently, I lead its Center for Data-Driven Policy, where we draw on our expertise on topics like acquisition and cybersecurity to bring objective, nonpartisan insights to policymakers.

Prior to joining MITRE, I was at GAO, where I worked closely with this Committee crafting FITARA, helping with the creation of the scorecard, and assisting in its bipartisan IT oversight. This included oversight of legacy systems. Memorably, I testified at a 2016 hearing on legacy systems when then-Chairman Chaffetz opened the hearing by waving an 8-inch floppy disk that was used on a backup nuclear command and control system.

We all understand what is at stake here. Critical Federal systems are operating with known security vulnerabilities and unsupported hardware and software. These legacy systems support important missions like wartime readiness and operation of critical infrastructure.

Before I get into the main points in my testimony, I first want to commend this Committee for its consistent and bipartisan oversight of cyber and IT issues over the past 10 years. This Committee's leadership has resulted in more secure and efficient Federal operations and considerable cost savings.

I have two overarching points to make this afternoon. First, despite recent calls for action on our Nation's critical legacy systems, the Federal Government's plans, budgets, and actions are not where they need to be.

Second, I think it is essential that Congress steps forward and takes the lead by putting in place legislation that requires prioritized inventories, related modernization plans, and actions to ensure progress against those plans. I would like to expand on each of these.

In late 2001, we published a paper that made several recommendations to Congress to update the 2014 Federal Information Security Modernization Act, known as FISMA, to meet the ad-

vanced threats posed by China, Russia, and nation states. One recommendation was to modernize legacy IT systems to reduce costs and vulnerability.

Last year, I testified at the FITARA 13 scorecard hearing and helped to author a paper published by the American Council for Technology-Industry Advisory Council, known as ACT-IAC, on evolving the FITARA scorecard. Both my testimony and that report recommended an IT modernization category be added to the scorecard.

Last year, Senators Maggie Hassan and John Cornyn introduced the Legacy IT Reduction Act of 2022, that required agencies to develop an inventory of legacy IT systems and a plan to modernize those systems.

And the current Administration has also highlighted the need to address legacy IT systems. Most recently, the White House and its National Cybersecurity Strategy called for OMB to develop a plan to accelerate IT modernization and specifically to eliminate legacy systems.

Despite the many calls to action, agency modernization plans and efforts to replace these systems have failed to keep pace. There are several reasons for this, including the complexity of upgrading older versions of software, a reluctance to accept the risks of transferring mission-critical processing off of mainframes to cloud solutions, a short-term focus driven by annual budgets, and the lack of executive branch policies and legislation calling for multiyear budgets to support modernization.

Congress has an opportunity to catalyze this needed modernization effort. My written statement contains 10 recommendations for OMB, Congress, agencies, and industry. The two recommendations for Congress are this: One—enact legislation similar to the Legacy IT Reduction Act of 2022, introduced last session in the Senate, and implement the FITARA scorecard recommendation, which includes adding a legacy modernization category to it.

The other recommendations call for OMB to apply more urgency to their directives and for agencies to apply AI and machine learning to extract information from legacy IT platforms.

In summary, the U.S. has long been a global leader in technology. We have the tools and the expertise required to modernize and improve our outdated government IT systems. What is needed now is leadership and action.

We look forward to working with you, Chairwoman Mace and Ranking Member Connolly. This concludes my statement. I look forward to your questions.

Ms. MACE. Thank you, and I will now recognize myself for five minutes. I want to thank you all for the testimony you submitted today, the feedback, your ideas, legislative and otherwise, and explaining why we are where we are today.

One of the interesting things, Mr. Walsh, about your testimony today was acknowledging that the Federal Government does not know, I guess, what all systems that we have, which is deeply concerning to me. I would think we have got contracts, we have receipts for the contracts we have, that we would have some way to track this. And I guess we do not have a system that tracks what software different agencies have right now?

Mr. WALSH. In some cases, yes, we are not accurately tracking, and in other cases it is the right hand not knowing what the left is doing. And in a third case I would add identifying something as legacy requires being familiar with what it is doing and not doing well, and in a lot of cases we are not doing a good enough job evaluating our own systems and figuring out what is working and what is not.

Ms. MACE. Gotcha. Thank you. And then compared to the private sector, Mr. Walsh, the Federal Government spends a great proportion of its IT budget operating and maintaining legacy systems rather than investing in new ones, and you have sort of a different perspective on this too. But do you believe it tends to make the Federal data that we have more vulnerable to cyberattacks because of that? What are your thoughts on that?

Mr. WALSH. So, in part, yes. As our systems get older they get more vulnerable, easier to hack, and certainly less secure, harder to maintain. The private sector spends less, has better technology, but they face different threats, right. In terms of cybersecurity, nation state actors are much more focused on us. They are still going after private sector, especially China, Iran, certain other bad actors like Russia.

Ms. MACE. Russia.

Mr. WALSH. But our legacy IT can afford to get older because we are trying to be responsible stewards of taxpayer dollars. I think, you know, as I said, having all the newest and the best tools works for private industry—you know, the big companies, Google, Microsoft, and the like—but I personally would not want all the newest tools to be at USDA. I want the tools that are right, that are doing their job well, and I want USDA to periodically look at them and make that evaluation. But having the newest flash-bang computers should not be something that the government entertains.

Ms. MACE. Thank you. And then as I mentioned earlier in my opening statement, the Federal Government employs about four times as many IT professionals over the age of 60 versus under the age of 30, and we seem to be doubling down on outdated technology and older hires. We actually had the Director of OPM here, and this is not your fault, but it was the worst witness we have ever had, I mean, ever. It was just terrible. And I was just shocked that she was able to even hold that position.

But when we look at that issue of hiring employees, we recently saw a report that GAO reported the Social Security Administration recently had to hire tech folks out of retirement to maintain its COBOL system. So, how can we, as a government that is so slow, that is so bureaucratic, that is so old, well, not literally, but literally and figuratively in the IT systems that we have, how can we assemble a younger, more tech-savvy workforce when, you know, in its most pressing need for experts that have obsolete software needs? And so, without such a workforce, how can we move forward? We have all these people retiring soon, in the next couple of years, and not hiring enough young——

So, what are some of your thoughts on how we address that challenge?

Mr. WALSH. So, in some cases we have already done, and your Committee has been a large part of this, given the flexibility to

agencies to try and find new ways to put money into IT and also try to find new ways to get more IT talent into the government, because you are absolutely right, we are facing a pending wave of Federal employees who are going to retire and take a lot of knowledge and expertise with them.

If we are going to avoid paying a premium to bring them back from the golf courses then we need to make sure that we have that next cadre of IT professionals coming.

Ms. MACE. And they do not need a college degree to do it either, right?

Mr. WALSH. Absolutely not.

Ms. MACE. Yes. A member of my family never went to college, makes more money than I do. He is 21 and owns his own home. I did this wrong. When I got out of school, programming, we were making $35,000 a year in the late 1990's, so much different perspective.

I have got one last question I did want to ask. FAA issues with legacy systems and the FAA legacy system failures, critical agency functions were on full display earlier this year when the FAA, in January, had to suspend flights because of a breakdown of a key computer system in my district at Hilton Head Island Airport. Outdated technology forces air traffic controllers to use binoculars, 1800s-level technology, to coordinate plane landings.

How many such critical Federal operations are running on outdated technologies like this, anywhere?

Mr. WALSH. Uncountable. Uncountable. Disappointingly. Enormous.

Ms. MACE. Yes. Thank you.

I would now like to yield five minutes to the Ranking Member, Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairwoman.

Ms. Kent, we talked about bipartisanship. You worked in what Administration as CIO?

Ms. KENT. I was appointed during the Trump Administration.

Mr. CONNOLLY. And did you find us cooperative in your endeavors?

Ms. KENT. I found this Committee to be engaging and cooperative as we sought ways, much like these challenges, to move forward.

Mr. CONNOLLY. All right. I do not want to ruin your reputation in certain corridors, but I thought it was a very productive relationship, and I am so glad to see you again, and thank you for your efforts to try to promote positive change within the Federal Government.

Why, your experience as CIO, why do not we just retire legacy systems? I mean, my refrigerator is old and I replace it, after 20 years, certainly after 60. So, why—you were CIO, what is your experience why Federal agencies do not do it?

Ms. KENT. Risk, cost, and resources. And I want to use a specific example that kind of harkens back to the last question. One of the TMF projects that we did was a project for HUD, and what they looked at was the fact that they had seven legacy systems, we started with three, that had seven million lines of COBOL code,

and that was written by a small group of individuals that were no longer able to help with any modernization efforts.

Mr. CONNOLLY. They were not even on the golf course.

Ms. KENT. They were not even on the golf course. They were not even available to show up at work.

And what they did was actually bring in technology to convert that 70 million lines of code to 1.2 million lines of Java. We used a tool. We tested the tool. The agency moved the capabilities. They managed the risks during that effort, and now we could hire new college grads because they were competent in Java.

And so, that is a great example of an agency stepping forward, they accepted the risk, they made the technology investment, and then they hired the people to sustain the path going forward, but not every agency chooses to be that bold.

Mr. CONNOLLY. I think you put it well—risks and costs, particularly.

Mr. Powner, from your days at GAO, it is a big deal to replace your legacy systems, and maybe upgrade your IT while you are at it. I mean, we are talking multibillion-dollar, multiyear kind of thing. For a manager to invest political capital in that endeavor is a big deal, and he or she may not be around to even see the fruits of that endeavor. And then, even though we spend $100 billion a year, 80 percent of it is spoken for. And so, I do need working capital, don't I, to try to decide to make this big decision.

Mr. POWNER. Yes, I think the key here is you need a long-term, multiyear focus to tackle these problems. The annual budget cycle does not help with that. And that is where I think legislation, if you could get focused on the right set of systems that we really need to tackle. I agree with Mr. Walsh that there are a lot of these systems out there——

Mr. CONNOLLY. But let me interrupt you, if I may, because I am going to run out of time. But is not that why Congress, led by my former Republican colleague, Will Hurd, on this Subcommittee, created TMF, to have working capital to try to incentivize people to go beyond the year-to-year——

Mr. POWNER. Yes, both TMF and the working capital funds in the MGTF were both two tools that you really want to use, as Ms. Kent mentioned, moving forward.

But I do think you need to prioritize inventory because we have so many of these things, and that is where I think the focus from Congress requiring that prioritized inventory that could be tracked, not only by the Congress but tracked by the Federal CIO, and also you could use the IT Dashboard for transparency. We need better light and focus on these things so that we can make progress on not only putting good plans in place, but eventually putting new systems in place.

Mr. CONNOLLY. Real quickly, Mr. Walsh, as the FITARA scorecard and 17 oversight hearings with respect to it, do you think made a material difference in incentivizing Federal agencies to upgrade their IT?

Mr. WALSH. Yes.

Mr. CONNOLLY. Save money?

Mr. WALSH. Yes.

Mr. CONNOLLY. Ms. Kent, same question.

Ms. KENT. It definitely placed focus and saved money, and as we have had many conversations in the past, it is like the IT question that we are talking about is we need to continue to advance what we measure and be very focused on the next challenge.

Mr. CONNOLLY. Absolutely. Mr. Powner, same question.

Mr. POWNER. Yes, it has, and I think it is important to evolve it to things like our workforce, like better metrics in the cybersecurity area, and legacy modernization.

Mr. CONNOLLY. Yes. And just let me end, Madam Chairwoman, I would be delighted to work with you in adding this legacy modernization category to the scorecard because I think we have got to have plans in place to finally retire legacy systems and a timeline and a budget for how we do that.

Thank you, Madam Chairwoman, and thank you again to our panel.

Ms. MACE. Thank you, Mr. Connolly.

I would now like to recognize Congressman Timmons from the great state of South Carolina, for your five minutes.

Mr. TIMMONS. Thank you, Madam Chair.

I have served as a prosecutor in a local district attorney's office. I have been in the state Senate, and I have been in Congress for a number of years, and this has been an ongoing question—how do we effectively modernize our IT to make sure that we are good stewards of the data that we have?

I think the bigger challenge is the government does not really have traditional accountability. Private businesses are fined or settle court cases for over $1 billion, hundreds of millions of dollars, so there is a free market incentive for what motivates them to protect their data.

We recently had the DC Health Exchange in. They are a hybrid, they are pseudo, quasi government, so it will be interesting to see how that plays out. The CFPB recently had a breach, and that was more user error, but that resulted in a 250,000 individuals' personally identifiable information to be leaked, which resulted in a lot of fraudulent unemployment claims, which, you know, it is very interesting what people do with data.

But again, this is just a major problem, and I want to talk about damages. What happens to the CFPB, what is the recourse for the individuals that have been aggrieved based off of a government breach, based off a government failure to protect data from individuals, in many cases that they force to interact with? Mr. Walsh, what is the recourse?

Mr. WALSH. You would hope that it would be like the private sector, as we have all received, I am sure, numerous notices that our data has been breached, that they would provide some assistance, but I am not familiar with what would happen if the CFPB were hacked.

Mr. TIMMONS. Well, we have had a lot of government data breaches. I mean, I do not see huge, hundred-million-dollar settlements from the government. We have sovereign immunity. You are not allowed to sue the Federal Government. You are not allowed to sue the state or local government. I mean, really, the recourse is likely people get fired. I mean, is that kind of the recourse?

Mr. WALSH. So, people could be fired. One would hope that people would be held accountable through hearings such as this today. But I would not want to speculate.

Mr. TIMMONS. Well, let us get to the root of the problem. I mean, we have servers all over the country that are extremely expensive to update. The training necessary to implement best practices as it relates to employees accessing data is not cheap. I am in the Air Force, and we do these ridiculous trainings on-line that is just really the bane of my existence when I got to drill.

But, I mean, the answer is eventually going to be cloud migration, and that should save money long-term, once we are no longer spending money on maintenance. I see, Mr. Powner, you are nodding your head. Is that fair?

Mr. POWNER. Yes. Clearly there could be long-term savings going to the cloud, but the thing with these legacy applications is during the transition you are running dual operations typically, so there is always an investment initially with savings down the road.

We talked about the IRS system. I mean, if we look at the individual master file you are going to have to run dual operations there for a while, and it is going to result in an investment.

Now long term, are you going to save on maintenance costs and those types of things? Yes. I mean, are you going to have better security? Yes. But there is going to be some investment during that transition that you are going to have to bite the bullet.

Mr. TIMMONS. I just tried to pay my Federal taxes, and it is extremely complicated, the dual factor authentication. It is effective. It just requires me to look back at historical taxes. If we had something like that during the pandemic for either PPP loans or for EIDL loans, or for unemployment claims, we would have saved, I do not know, half a trillion dollars?

So, I mean, we are already seeing the costs of not having—I would not even call that best practice. That is just basic. Dual factor authentication to confirm the user's identity that is accessing a government system is so basic that it is shocking that we do not have it. And because we did not have it at SBA, it cost half a trillion dollars. I mean, any guess what it would have cost two years ago, or let us just say before the pandemic, three or four years ago, to make sure that SBA used dual factor authentication? Probably less than $1 billion. Maybe a couple hundred million? What do you think? Mr. Walsh?

Mr. WALSH. That certainly seems reasonable for a couple hundred million.

Mr. TIMMONS. So, we could have spent a couple hundred million dollars to save half a trillion. And I think that we are just seeing the beginning of this. We are going to continue to have increasing frequency and degree of breaches or of uses where it would have benefited greatly.

So, I appreciate that you all are here testifying before us. This is very important, and we need to keep working on it.

With that I yield back. Thank you.

Ms. MACE. Thank you.

And I would now recognize Mr. Lynch for five minutes.

Mr. LYNCH. Thank you, Madam Chair. Thank you for holding this hearing, and thank you and the Ranking Member, and thank

you to our witnesses for your willingness to help the Committee with its work.

So, as the Ranking Member pointed out earlier, we are spending about $100 billion a year on cyber systems, although 80 percent of that, $80 billion, is actually going to maintain legacy systems that we are supposed to be converting. Is there a system in place where we automatically say, "OK, this system has been in place since 1973, and we are getting rid of it" or is it left up to the individual agency to adopt a program of modernization and going to a more robust system?

Mr. WALSH. So, there is no such system that says just because it is old we need to retire it. In fact, just because it is old, I think we should do an evaluation, but there may be good cases where it does not make sense from a benefit perspective or even a cost perspective to retire something just because of age.

Mr. LYNCH. Yes. I know I read a report by, I think it was the FBI, that said that right now we are outnumbered like 50 to 1 in terms of—even if we put everybody on cybersecurity in the U.S. Government just on China, the number of hackers would outnumber us like 50 to 1. That is just with China.

And I am concerned that if we do not change up the way we are doing things here, even the most, I guess, ordinary systems are now targets of Chinese hackers, right? They said that they actually hacked the Merit Systems Board as well, which basically just handles Federal employee complaints and fairly mundane issues. But there is so much hacking going on, even those more mundane systems that we would not consider as threatened or as important as others, they are actually targets.

So, I do not know if we can afford to leave any legacy system that is porous in place, and I think it is a sign of inattention or lack of priorities that I have been coming to these meetings, these hearings, for about 20 years, and yet we seem to be going over the same ground again and again. And there is no robust system for changing this out, and I am searching for a way to make that happen.

I know it will be painful for some of these agencies. I know that in many cases employees might be comfortable with a legacy system. They know how that operates. It would require them to train themselves on a new system. But I think it is necessary for the national security of this Nation.

And I am just wondering if you have any—I mean, you have been dealing with this up front every single day for a long, long time. What are your recommendations that we might light a fire under some of these people to make them, you know, adopt the modernizations that are necessary?

Mr. POWNER. Well, I clearly think there needs to be more consistency agency-to-agency on how we tackle legacy issues. And you mentioned these major security vulnerabilities, and I think Representative Timmons brought up, you know, not being able to use multi-factor authentication. Well, many of these legacy systems make it difficult to use multi-factor authentication. That is a tenet of what we are trying to go toward with zero trust, with cybersecurity.

So, I would start with the legacy systems, and we could talk about unmet mission needs, we can talk about high maintenance costs. But if you have a security vulnerability, that needs to be right at the top of the list. I think a prioritization criterion should come from OMB. I am not saying Congress needs to come up with the criteria, but I think Congress and legislation should direct OMB to have prioritization criteria so that we have more consistency, Representative Lynch, and would better address the key points that you are making.

Mr. LYNCH. Do we have the ability to say, OK, a system that is being used by a certain department is not capable of delivering zero trust compliance under the President's initiative? Is there an ability to rule some of these systems out that are not capable of compliance, and get rid of those?

Mr. POWNER. You would have to go to, probably, each individual agency and have that discussion with their CIOs and CISOs. But the answer is you could do that, yes.

Mr. LYNCH. OK. All right. Thank you for your courtesy, Madam Chair. I yield back.

Ms. MACE. Of course.

I would now like to recognize Congressman Burlison for five minutes.

Mr. BURLISON. Thank you, Chairwoman. I am going to try to rapid fire some questions here. I have been here four months, so I am just trying to get my head wrapped around how we do IT at the Federal level. So, can you give me an idea, do different agencies, do they have full control? Do they stand up their own IT departments and have their own funding? Do they make decisions unilaterally without context?

Mr. WALSH. So each agency, yes, in the majority of cases, has its own IT department, and in addition, agencies that have components or bureaus may also have their own bureaus or departments.

Mr. BURLISON. And within those you have got—do you have programming teams?

Mr. WALSH. You have programming teams. You have contractors. You have CISOs, the whole gamut.

Mr. BURLISON. How many different, of the products that we manage, or within the Federal Government, given a particular agency—and this may be hard to answer—but how much of it is in-house programmed versus vendor purchased?

Mr. WALSH. So, I know that we would be heavily in favor of the government using COTs, commercially off-the-shelf software, or GOTs, government off-the-shelf software, but I do not know of any specific study that has identified government-wide what the mix of contractor-built versus government-built is.

Ms. KENT. And Kevin, if I might add, sir, to your question. It varies agency-to-agency. Some agencies, they significantly have a staff that looks over their set of technology products. Others do leverage outside sources more significantly.

And to your first question, each agency is actually charged with managing their own technology environment, and those are responsibilities that are tasked on the CIO. But the priority discussion that we have been having is the head of agency, and when it comes to how they operate, that is the responsibility of the CIO, but the

funding priority and the initiatives—because many of these technology implementations impact operations and they impact mission —are an all-of-agency decision. So, those things impact the pace of how the various agencies move forward.

Mr. BURLISON. Do any of the agencies decide to outsource the entire departments or the sections of IT?

Ms. KENT. Agencies use services provided as a service, but for various different things—we have had cloud discussions, you know, multiple times, so that may be an example. But that does not absolve them of any of the responsibility for managing that technology or managing the risk. That is completely the responsibility of the agency, and that is why the choice of their partners is so important.

Mr. BURLISON. So, do you find, or is there opportunities for, you know, cost savings or economies of scale, where different agencies can leverage the same software?

Mr. WALSH. So, the government does some of that——

Mr. BURLISON. No?

Mr. WALSH [continuing]. With its Shared Services Initiative, where they try to bundle, you know, multiple different agencies together.

Ms. KENT. I am only smiling because one of the Shared Services Initiatives was during the time that I served, and we were extremely focused on it. It is a perfect example of some of this legacy discussion. The mission support services, things like payroll and grants management, things that are done, some of our financial capabilities, they are done commonly across the entire Federal Government and governed by the same law. Yet, we have 124 time-and-attendance entry systems across the government.

Mr. BURLISON. Yes, ridiculous.

Ms. KENT. So, do have opportunity, but migrating is expensive and risky. And so that is why, you know, we have seen slowness in moving to some of those centralized capabilities and——

Mr. BURLISON. And I imagine these agencies, they do not want to give up the power that they have over this particular software. That is what I have seen in large-scale companies.

Ms. KENT. Yes, sir.

Mr. BURLISON. You have got different silos that they just want to control that silo.

But my question to you is, since we are in the positions that we have, can we implement policy that forces that integration and that economy of scale?

Ms. KENT. I think there are certainly opportunities for that, and you looked at shared services as one. And we have a list of legacy systems——

Mr. BURLISON. And then before my time is up I wanted to ask, you know, I remember studying the CHAOS report from the 1990's, project management. Most IT projects are nothing like construction projects in that within IT there is a significant failure rate, cost overruns, over time, over budget. Around 45 percent of projects are successful. What is the success rate within the Federal Government, across the board?

Mr. WALSH. So, I cannot give you an exact number on what that is right now. We have not done that work. But I do think that the

advent of modern techniques to do software development has helped lower that number, things like agile software development, where you can hopefully, if you are going to fail, fail sooner, without wasting billions of dollars.

Ms. KENT. Sir, I would add that the projects that are under the Technology Modernization Fund, there have only been two that have not hit their timeline, and there have been zero that had cost overruns, because those are being managed using a more comprehensive and modern project process.

Mr. BURLISON. OK. Thank you.

Ms. MACE. Thank you.

I will now recognize Mr. Langworthy for five minutes.

Mr. LANGWORTHY. Thank you, Chairwoman Mace.

Legacy IT systems continue to plague both our state and our Federal Governments, and this was made very evident by the challenges that my home state of New York faced in the Department of Labor during the COVID pandemic. The Department struggled to issue payments in a timely and efficient manner due to its reliance on an outdated technology. And even more so, it issued an estimated $11 billion in either improper payments or fraudulent payments.

Despite ongoing efforts to modernize, that Department still faces significant hurdles due to legacy complications.

Ms. Kent and Mr. Walsh, the Cyber Security Strategy paints a pretty dire picture when it comes to the elevated cyber risks we have in the Federal Government due to all of the legacy IT systems at our agency levels. Now specifically, you know, what do agencies need to do to address the legacy IT problem, and how can we, as a government, accelerate the migration to cloud-based services?

Mr. WALSH. So, to address the legacy IT problem I think first we need to figure out where it is. Every agency needs to have a good understanding of what their systems should be doing, evaluate them, see if they meet the mark, and if they do not, maybe it is time to think about that retirement or replacement.

To the example you referenced where the State Department of Labor had troubles issuing payments for its unemployment insurance, I think that was a case of unanticipated capacity. During COVID, they had to suddenly ramp up, which, as you pointed out, cloud computing, where you can buy capacity on demand, is a lot easier to absorb that massive influx of capacity that may be unplanned for.

So, I think migrating to more modern data platforms would be another step that you could take to address that.

Ms. KENT. I would only add to that, sir, making it a priority. And you heard the example of unanticipated capacity needs, but moving into that environment was also not funded, and had not been funded because there was not a view that that capacity was going to be needed. New York was not alone, with other states who kind of had that same approach.

So, a plan that continues to look forward and take advantage of modern technology capabilities that gives you scale and resilience should be a path that not only are we on at the Federal agencies, but also our state and local government, you know, partners that deliver those services.

Mr. LANGWORTHY. Mr. Walsh, in the past few years GAO has written numerous reports regarding shared services, including the significant government cost savings of consolidating HR, payroll, financial services across the Federal Government, many of which rely on legacy and outdated technology systems.

Can you provide a brief update on how agencies are doing in terms of modernization and consolidation with respect to implementation goals and milestones for agencies to transition from one provider to another?

Mr. WALSH. So, I do not have that information with me today, sir. I can take that question for the record, though.

Mr. LANGWORTHY. Thank you. Thank you very much.

And Ms. Kent and Mr. Walsh, what should Congress be doing to address the challenge of IT modernization besides holding hearings like this? Are there specific legislative proposals that we should be thinking about, such as requiring agencies to inventory legacy IT or submit modernization plans?

Mr. WALSH. Absolutely, and I think a good starting point would be OMB's 2016 draft guidance that was never finalized. If that were finalized, I think that would be a great starting point. In our 2018–2019 report, we also flagged some of the most important legacy systems in need of modernization. I think those would be a great starting point, although I would hope the agencies have been tracking and updating that list since then.

Ms. KENT. And, sir, as I referenced in the opening statement, some agencies do have plans for modernization, and at times they have been submitted, and there is not a realism about the budget because in many cases, while you are supporting a legacy system and building a modern system, you are duplicating your costs. So, being realistic about that process.

Other agencies have not even built a plan, a realistic plan, that has cost estimates and an anticipated timeline. So, that is an opportunity for Congress to push harder.

Mr. LANGWORTHY. And just in my last remaining time here, are there regulatory or policy hurdles that make a transition to a cloud-based service challenging for the government?

Ms. KENT. There are—yes and no. All agency CIOs are accountable for the risk and the performance for their particular agency. So, as another Member asked a question, you cannot outsource your risk. So, in making those choices there are services available—it is still incumbent on that particular agency to do work to ensure that that is not a risky environment. Are the services available and are they available commercially? In most cases, yes.

Mr. WALSH. Just to add, in addition to the risk as you making the go/no-go decision on the modernization, making sure that you are comfortable with the risks that the contractor or cloud service provider is taking to protect the government's data is something else that we need to keep focused on, making sure that whether that is citizens, you know, taxpayer data, whether that is data from the Department of Education on Federal student loans, or IRS, we need to make sure that those data are adequately protected.

Mr. LANGWORTHY. Thank you for your time and your testimony today. I yield back, Madam Chair.

Ms. MACE. Thank you.

And I would now like to recognize Mr. Edwards, from North Carolina, for five minutes.

Mr. EDWARDS. Thank you, Madam Chair. To our witnesses, thank you for your time this afternoon and for your service to help out our great country.

Ms. Kent, one of the things that you mentioned earlier that really interests me because, while serving in the North Carolina Senate, I served on our state's IT Committee, and this issue was very much at the forefront, particularly because so many of our systems were built on COBOL, and in a lot of cases we had a hard time finding people alive that could work on COBOL.

But you mentioned a situation where an agency converted 1 million lines of COBOL code to Java. I have never heard of that practice before. So, can you tell us a little bit, how practical is that, just plugging it in and letting it translate? How reliable is it? How expensive is it? Do you save any money when you use that process relative to just starting out with a blank hard drive?

Ms. KENT. I am going to try to answer all of those questions, and I am going to start with is there a process and are there reliable tools. Much like Chairwoman Mace, I started my career in financial services, and there are definitely tools that are capable of making those types of transitions, with these points. It was 7 million lines of COBOL into 1.2 million, approximately, of Java. The tools that were used and tested in that process got about 70 percent of it right. So, there still had to be some hands-on work with people who understand the business processes of the agency to address those things that are not an easy fit.

There are many automation tools today that are proven, have been proven by multiple industries, that can perform at a similar level. The expense, you can save because you now did not go hire all those COBOL programmers that everyone is fighting over, and you used a technology tool, but you cannot bypass the fact that you have to have skilled resources that understand the business and mission processes in those agencies to take it the last mile and manage the implementation.

Mr. WALSH. If I may, sir, there is also currently the development of artificial intelligence, AI, and some of the tools that the Chairwoman mentioned earlier, the impact that those are going to have on the ability of the government to manage its legacy IT is going to be very interesting to watch in the coming months. That may be a significant force multiplier, making it easier to do those kinds of efforts, where you translate old code that no one can maintain or update anymore, and you use the AI to translate it into something that is easier to work with.

Mr. EDWARDS. Thank you for that. And so, let us be realistic. What we need to do to modernize is appropriate more money. I mean, it is going to take resources. However we choose to verbalize it, that is what it boils down to. And we do not have unlimited resources. We do have to be responsible with the taxpayers' dollars. And so, I foresee that there would need to be some level of prioritization.

Do you know, has there been a process put in place to prioritize the agencies where we begin? If so, where do we find that

prioritization, and if there is not, how do we go about prioritizing the agencies that we need to fund first to modernize?

Mr. WALSH. So, I would add a nuance there that I would not focus on modernizing an agency. I would identify specific systems that can bring the most benefit or are the most risky and prioritize funding toward them. But I think the process to identify all of the legacy systems, and then prioritize, is one that we can focus on, and legislatively, maybe, a solution for you to explore.

Ms. KENT. And sir, I might add that more focus first, because in some cases modern technology is actually going to save money, effort, or improve the mission of the agency. And an example may be, in one particular department we modernized all the forms and processing and an exchange process between three different Federal agencies, and what that meant in that efficiency is that we did not have backlog and we did not have calls coming into their support centers.

So, we actually saved money. It did not appear in the IT budget, but the agency itself saved significant money and delivered on their mission much better.

Mr. EDWARDS. Thank you. Madam Chair, I yield.

Ms. MACE. Thank you, Mr. Edwards.

This concludes our hearing this afternoon. In closing, I want to thank our panelists once again for their testimony today. I know there are many different tools and applications that they are using in the private sector and public sector for converting COBOL to Java. Thank you for bringing up that example.

I know folks that use GitHub Copilot to program. They get about 70 percent of their code from it and then they have got to manually do the rest of it, as you mentioned in your example. But I guess about a year ago Copilot also announced that they could take COBOL code and make it into Java using a couple of tools that they have, but there are others, CloudFrame, there are many different other tools. So, thank you for using that as an example.

And as I said in my opening statement, we are going to be introducing legislation to help improve modernization efforts with IT legacy systems. This hearing has reinforced this sort of need for these kinds of bills and legislation, so we appreciate your feedback. And we look forward to continuing our conversation as we work together, and to do that, and putting that together.

Before we adjourn, I ask unanimous consent to enter into the record the U.S. Chamber of Commerce statement and letter. Without objection, so ordered.

Ms. MACE. And with that, without objection, all Members will have five legislative days within which to submit materials and submit additional written questions for the witnesses, which will be forwarded to the witnesses for your response.

If there is no further business, and without objection, we are adjourned.

[Whereupon, at 3:16 p.m., the Subcommittee was adjourned.]

○