S. Hrg. 117–38

CONTROLLING FEDERAL LEGACY IT COSTS AND CRAFTING 21ST CENTURY IT MANAGEMENT SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

APRIL 27, 2021

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
45–043 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

David M. Weinberg, *Staff Director*
Zachary I. Schram, *Chief Counsel*
Pamela Thiessen, *Minority Staff Director*
Andrew Dockham, *Minority Chief Counsel and Deputy Staff Director*
Laura W. Kilbride, *Chief Clerk*
Thomas J. Spino, *Hearing Clerk*

SUBCOMMITTEE ON EMERGING THREATS AND SPENDING OVERSIGHT

MAGGIE HASSAN, New Hampshire, *Chairman*

KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
JON OSSOFF, Georgia

RAND PAUL, Kentucky
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

Jason Yanussi, *Staff Director*
Allison Tinsey, *Counsel for Governmental Affairs*
Greg McNeill, *Minority Staff Director*
Adam Salmon, *Minority Research Assistant*
Kate Kielceski, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, APRIL 27, 2021

ALPHABETICAL LIST OF WITNESSES

APPENDIX

CONTROLLING FEDERAL LEGACY IT COSTS AND CRAFTING 21ST CENTURY IT MANAGEMENT SOLUTIONS

TUESDAY, APRIL 27, 2021

U.S. SENATE,
SUBCOMMITTEE ON EMERGING THREATS AND
SPENDING OVERSIGHT,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10 a.m. in room 342, Dirksen Senate Office Building, Hon. Maggie Hassan, Chair of the Subcommittee, presiding.

Present: Senators Hassan, Sinema, Rosen, Ossoff, Scott, and Hawley.

OPENING STATEMENT OF SENATOR HASSAN[1]

Senator HASSAN. Good morning, everybody.

I want to start by thanking all of our witnesses for appearing today to discuss controlling Federal legacy information technology (IT) costs and crafting 21st century IT management solutions. I also want to thank Ranking Member Paul and his staff for working with us on this hearing and for our continued partnership to address wasteful spending and government inefficiencies. Even though Ranking Member Paul is unable to join us this morning, I look forward to addressing the threats posed by the Federal Government's failure to maintain a modern and agile information technology infrastructure.

Today is the first of multiple hearings on Federal legacy IT systems. By shining a light on this important issue, I hope that agencies will work to reduce their reliance on costly legacy IT systems, in partnership with Congress, the Biden administration, and industry stakeholders.

Today's hearing will focus on identifying the costs and consequences of legacy IT, as well as the institutional barriers to modernization. According to the Office of Management and Budget (OMB) and Government Accountability Office (GAO) , in fiscal year (FY) 2020, the Federal Government spent nearly $90 billion on IT investments and operations. Based on analysis of agency expenditures, legacy IT maintenance costs accounted for one-third, about $29 billion, of that total spending. However, the actual cost is esti-

[1] The prepared statement of Senator Hassan appears in the Appendix on page 29.

mated to be much greater when we consider legacy IT's negative effects on security, delivery of services, and customer experience.

To frame our discussion we should have a common definition of legacy IT. The term "legacy IT" describes the Federal Government's use of old technology or custom systems designed to support insular agency operations. That is, legacy IT includes technology and systems that are no longer supported by industry vendors, as well as those that require additional maintenance or specialized knowledge to operate.

We have seen the consequence of relying on legacy IT systems. For example, in 2014, hackers stole the personal information of more than 20 million people from the Office of Personnel Management (OPM), because they were able to breach OPM's vulnerable legacy IT systems that lacked encryption. Despite this breach that was clearly linked to a failure to modernize, OPM still relies on a 34-year-old legacy IT system that costs $45 million annually, roughly one-third of OPM's annual IT budget, even though a modern system would only cost $10 million and produce $16 million in cost savings.

At the Internal Revenue Service (IRS), the system used to annually process millions of tax documents is more than 50 years old, and relies on a programming language called the Common Business-Oriented Language (COBOL), which was invented in 1959. In 2018, implementation of the 2017 tax law hit a major roadblock due to a shortage of staff with the specialized knowledge needed to update COBOL-based tax processing systems. IRS estimates that it costs $15.9 million annually to operate this system, and 60 percent of those costs are for labor alone.

During the coronavirus disease 2019 (COVID–19) pandemic, IRS faced additional challenges because many of its aging systems rely on paper rather than digital records, paper that was inaccessible to IRS employees who were working remotely. As a result, the American people felt the burden of delayed tax returns and economic stimulus payments.

Similarly, in 2016, the Social Security Administration (SSA) was forced to rehire retirees to maintain the COBOL system used for making payments to beneficiaries and their dependents. These systems cost the Social Security Administration about $146 million annually to operate. However, the Social Security Administration estimates that it would only cost $25 million over 5 years to modernize the system, and that would significantly improve functionality and security as well as eliminate the need for specialized programmers.

This begs the question, what are agencies waiting for? What is holding them back from realizing significant cost savings, increasing security, and providing greater customer service delivery through reducing their reliance on legacy IT?

In addition to the costs and consequences of relying on legacy IT systems, today's hearing will also discuss the institutional barriers that prevent agencies from moving forward with their modernization efforts. Our distinguished panel includes the Director of the Government Accountability Office's Information Technology and Cybersecurity team, as well as three former Federal agency Chief Information Officers (CIOs) who navigated the challenging IT modernization landscape and successfully moved their agencies away from legacy IT systems. I look forward to hearing from all of our witnesses about how they achieved success by leveraging available resources and by being innovative.

Now we are going to move to the testimony of our witnesses, but before we do that it is the practice of the Homeland Security and Governmental Affairs Committee (HSGAC) to swear in witnesses. If you will all please stand, including our one witness who is remote, and raise your right hand.

Do you swear that the testimony you give before this Subcommittee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. WALSH. I do.

Ms. COLEMAN. I do.

Ms. WYNN. I do.

Mr. EVERETT. I do.

Senator HASSAN. Thank you. You may be seated.

Now we are going to start with the testimony of each witness, and I will introduce each witness and then they will go forward with their testimony.

We will start with Kevin Walsh. Our first witness today, Mr. Kevin Walsh, is Director of the Cybersecurity and Information Technology team at the Government Accountability Office. He led the team that identified the 10 Federal legacy IT systems most in need of modernization. Mr. Walsh has 15 years of experience at GAO, where he has led reviews of chief information officer authorities, management of legacy IT systems, and assessments of IT-related risks.

Welcome, Mr. Walsh. You are now recognized for your opening statement.

TESTIMONY OF KEVIN WALSH,[1] DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WALSH. Chair Hassan, Ranking Member Paul, and Members of the Subcommittee, thank you for inviting GAO to testify on this important issue.

Generally, we envision legacy systems as archaic government computers, stuffed in a basement with fluorescent lights dismally flickering above, or perhaps in the warehouse next to Indiana Jones' Arc of the Covenant. While we do not need Harrison Ford for any IT systems that I am aware of, there are certainly government systems that are in desperate need of modernization.

In our 2019 report on the topic, we asked agencies about their critical legacy systems that were most in need of modernization. In total, the agencies identified 65 systems which were, on average, about 24 years old. These systems support some of the most critical functions in government, such as wartime readiness, student loans, the operation of dams and power plants, tax processing, and Social Security payments.

We took a deeper dive into the 65 systems and flagged the 10 systems that we thought were the most vulnerable and in need of

[1] The prepared statement of Mr. Walsh appears in the Appendix on page 31.

modernization. Some were operating with known vulnerabilities or were written in older code, such as COBOL or assembly languages, and others had hardware or software that was no longer supported by the vendor. As the recent hacks of the software supply chains demonstrate, we have no shortage of bad actors in the world willing to take advantage of vulnerabilities like these.

We also asked the agencies that owed these 10 systems some very basic questions. Do you have a modernization plan? Does your plan include timeframes, a description of the work, and a plan to turn off the older system? Disappointingly, only the systems at the Department of Defense (DOD) and the Department of Interior (DOI) had these things in place. Further, there were no modernization plans for the systems at the Department of Education, the Department of Health and Human Services (HHS), and the Department of Transportation (DOT).

To be fair, the hardware these systems ran on was not as old as their software. The hardware averaged a bit over 7 years old. However, to put that in context, Amazon made news early last year when it extended the useful life of its servers from 3 to 4 years.

In general, as our servers get older, and our systems with them, 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. Basically, we are balancing cost, staffing, security, and functionality.

To keep the lights on and systems running, we are accepting risks that, in hindsight, may not make sense. For example, as the Chair noted, OPM reported that some of its networks were too old to implement encryption, a rather important security step.

Looking forward, modernization decisions need to carefully consider the following: how risky it is going to be, including risks to security and privacy; the criticality of the system; the cost to modernize or maintain the current system; potential cost savings; whether mission needs are being met; and if additional functionality or performance can be gained.

After considering all of that, there will undoubtedly be instances where modernization may not make sense. For example, National Aeronautics and Space Administration (NASA) uses Fortran code to communicate with the Voyager space probes that we launched in 1977. We cannot catch and upgrade that hardware.

On the other hand, we also identified a system at the IRS that reported annual labor and operating costs of about $16 million. The IRS reported that it would cost a staggering $1.6 billion to upgrade that system.

We have also noted that agencies may not have a complete picture of their legacy systems. OMB drafted guidance in 2016, that would have required agencies to identify, evaluate, and prioritize their IT investments to make modernization decisions. Sadly, that guidance was never finalized.

Until agencies are able to identify all of their legacy systems, assess them, and document their plans for modernization, they run the risk of wasting money on systems that are not meeting mission needs or are likely putting the agencies at risk.

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

Senator HASSAN. Thank you very much. Next we will move to Casey Coleman. Ms. Coleman is the Senior Vice President for Digital Transformation at Salesforce. In this role, she is responsible for developing strategies and solutions for government customers looking to modernize their IT systems. Prior to joining Salesforce, Ms. Coleman served as the Chief Information Officer at the General Services Administration (GSA), where she led several modernization initiatives, including the first agency-wide move to cloud-based email and collaboration platforms. She also led Federal efforts to develop the FedRAMP standards for cloud services and cybersecurity.

Welcome, Ms. Coleman. You are now recognized for your opening statement.

TESTIMONY OF CASEY COLEMAN,[1] FORMER CHIEF INFORMATION OFFICER (2007–2014) AT THE U.S. GENERAL SERVICES ADMINISTRATION

Ms. COLEMAN. Thank you, Chair Hassan, Ranking Member Paul, and Members of the Subcommittee for the opportunity to speak on today's important topic. It is very timely, because we have been talking about modernizing Federal IT for a long time, and it has been a priority, but the prospects for progress have been significantly improved with the emergence of modern, cloud-based digital platforms. The world's largest banks, manufacturers, retailers, and health care companies are already transforming their operations and customer service by embracing the cloud. The Federal Government can do the same.

All of us engage with the government through interactions like paying taxes, adhering to regulations and laws, and receiving benefits and services, and IT has become the critical enabler to carry out vital missions of the government, such as defending the Nation, providing economic stability, and improving public health. It is in all of our best interests that government and its IT systems work well.

But too often legacy IT is not an enabler but a concrete barricade, making the experience for employees and customers fragmented, opaque, and confusing. When I first came into government I was surprised to see how our systems did not work for us. We worked for them. I could not believe how the technology slowed us down and frustrated our efforts to collaborate. These are commonplace issues, and they do not really inspire trust or confidence.

Meanwhile, in our personal lives, as consumers and customers, everything is online and mobile, personalized and accessible any time. We expect the same of government, but this creates a growing gap between what we expect and what is being delivered.

The COVID pandemic really highlighted this growing gap. This was a crucial moment of need, and the organizations that delivered successfully, public sector and private, were those that moved to the cloud, so their employees could work from anywhere and deliver services online. We saw years of modernization compressed into a few months, from telehealth services to paycheck protection loans, employee wellness checks, and contact tracing.

[1] The prepared statement of Ms. Coleman appears in the Appendix on page 72.

These programs were not on anyone's radar before the pandemic, so what made the difference? Moving to the cloud, with access to rapid innovation and secure online services from the commercial platforms already serving the world's largest companies.

Why does this matter? For a farmer, they can get their crops in the ground by not getting off the tractor and going into town to get their crop loan but rather by doing it through a mobile app on their phone, not wasting time. For a veteran seeing their doctor by video means they continue to receive the treatment they need and the benefits they have earned.

This pivot is important for government employees as well. No one comes into the government to step backward in time and do things the old way, with brittle tools that were state-of-the-art decades ago. They want to serve a mission and make a difference. If we want to recruit and retain talented public servants who have a choice, we have to give them tools to empower them and make their work effective.

I am especially passionate about this because I have seen it firsthand. As the CIO for GSA through much of the Bush and Obama Administrations, I had the privilege of leading a multiyear modernization program to move GSA to the cloud and improve service delivery. When the Obama Administration announced the Cloud First policy, we led the way, becoming the first to move the entire agency to cloud platforms for email, collaboration, and productivity tools.

Our previous system was on really old hardware. We did not know when it went down. I used to send myself emails at nights and weekends to make sure it was still working. By moving to the cloud, we had all our tools available anytime, anywhere, and when weather emergencies like Superstorm Sandy shut down all Federal offices, GSA kept going, working remotely as they have through the pandemic.

In closing, modern cloud platforms are a complete game-changer for improving government service delivery and mission execution. I do not mean to suggest this is a silver bullet, and I have included recommendations in my written testimony for other reforms, but all of these factors only click when you add the cloud.

Thank you, and I look forward to questions.

Senator HASSAN. Thank you, Ms. Coleman.

We are now going to turn to the witness who is joining us remotely, Ms. Renee Wynn. Welcome, Ms. Wynn.

From 2015 to 2020, Ms. Wynn was the Chief Information Officer for the National Aeronautics and Space Administration. She retired from NASA last April following a 29-year career in Federal service that included 9 years spent in Federal information technology. During her time at NASA, Ms. Wynn was a critical and creative leader in the formulation and implementation of the Modernizing Government Technology (MGT) Act, and she worked on several projects to reduce the agency's reliance on legacy IT system. She now operates her own consulting firm.

Welcome, Ms. Wynn. You are now recognized for your opening statement.

TESTIMONY OF RENEE P. WYNN,[1] FORMER CHIEF INFORMATION OFFICER (2015–2020) AT THE NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Ms. WYNN. Good morning, Chair Hassan, and distinguished Members of the Subcommittee. I am honored to be here to testify today on the importance of IT modernization. Now is an ideal time for departments and agencies to focus on large, complex IT modernization projects. Many lessons have been learned about remote working and delivering Federal services during the COVID pandemic. These lessons can be used to accelerate modernization efforts. This, combined with having the right personnel, processes, and budgets significantly increase the probability that such projects will be successful.

As the former Chief Information Officer at NASA, and the Acting CIO and Deputy CIO of the Environmental Protection Agency (EPA), I have had ample opportunity to understand the dynamics inherent in modernizing IT. These experiences gave me the best view of the biggest challenges a CIO faces when modernizing IT—an agency's culture, or sometimes referred to as "the people challenge."

A CIO must have sustained support and funding for IT modernization from the agency heads, including her executive team. She must have the right people with the right skills, and she must build and maintain relationships across the agency and with the contractor community. Without this, complex IT projects will fail.

When I was offered a position at NASA, I was over the moon with excitement at becoming a member of this iconic Federal agency. I was confident that I would find best-in-class IT management and cybersecurity practices. What I found was a work in progress—a need for more centralized or enterprise-wide IT services, systems in need of modernization, a poor cybersecurity posture, and a culture that viewed the NASA CIO with skepticism.

Fortunately, NASA recognized this as well and had already completed a business services assessment (BSA). The BSA was undertaken to identify organizational and management improvement areas for NASA's mission support services, including IT. Based on the BSA recommendations, the CIO office developed and executed an implementation plan.

Many valuable lessons were learned, and a big issue was identified, which was preventing NASA from gaining the full benefit of the BSA. Too much of NASA's IT budget and staff were not managed by the NASA CIO, making it difficult to modernize IT and control spending. Given this, NASA took the bold and politically charged step of having all the people and budget associated with a mission support function report to the head of that function.

As I led the BSA implementation, the culture or people challenges were a constant. While NASA's top executives provided steadfast report, executives and staff below them were resistant and, at times, difficult. Nothing rattles a civil servant more than having portions of their budgets and staff reallocated.

Congress has taken the steps to address IT management and cybersecurity risks through legislation, from the Clinger-Cohen Act to

[1] The prepared statement of Ms. Wynn appears in the Appendix on page 86.

the Federal Information Security Modernization Act (FISMA) and on to the Federal Information Technology Acquisition Reform Act (FITARA). All were designed to advance IT in support of government services and provide improved information security. Support continued with the passage of the Modernizing Government Technology Act. This provided financial resources to agencies through the creation of a centralized modernization fund, called the Technology Modernization Fund (TMF).

The oversight of Congress has also been a driving factor in making the intended improvements to IT modernization and cybersecurity. Legislative actions, combined with sustained oversight, have provided the foundation to improve IT management and cybersecurity.

I will conclude today by emphasizing Congress should continue to hold oversight hearings and provide predictable funding and be prepared to act should gaps emerge in the Federal Government's ability to deliver more modern and effective public services. The CIO must have sustained support and budgets, plus a knowledgeable and skilled workforce, to meet the growing demands of IT modernization and cybersecurity. With this, the CIO can lead agencies forward to deliver IT modernization and improve cybersecurity so departments and agencies can deliver the mission for the American public.

Thank you again for the opportunity to appear before the Subcommittee today, and I stand ready to answer your questions.

Senator HASSAN. Thank you very much, Ms. Wynn. Now let's turn to our last witness, Mr. Max Everett.

Mr. Everett served as Chief Information Officer at the Department of Energy (DOE) following a career in IT security and risk management. During his time at Energy, Mr. Everett secured one of the first awards from the Technology Modernization Fund to migrate Energy's legacy email system to a cloud platform. He is now CEO of Adnovem Consulting Group, which works with public and private customers to provide services and promotes a lean and agile approach to IT modernization.

Welcome, Mr. Everett. You are now recognized for your opening statement.

TESTIMONY OF MAX EVERETT,[1] FORMER CHIEF INFORMATION OFFICER (2017–2020), AT THE U.S. DEPARTMENT OF ENERGY

Mr. EVERETT. Thank you, Chairwoman Hassan, Ranking Member Paul, and Members of the Committee. I appreciate the opportunity to be here this morning and talk about this. I appreciate the advocacy that you all are providing, and the support to all the CIOs who are currently going through the challenges of this. I would like to talk for a few minutes, after 20 years in and around Federal IT, to talk a little candidly about some of the challenges we have seen.

The events of the last year have obviously shown the critical importance of our IT and the challenges of legacy, whether that was

[1] The prepared statement of Mr. Everett appears in the Appendix on page 91.

supporting people impacted by COVID or some of the recent cybersecurity incidents that we are still grappling with.

I would begin here suggesting, as a few people have talked about, that it is important to talk about what constitutes legacy IT, and I think it is a broad definition. It is not merely the electronic systems. Fax machines are probably the most common legacy IT in the U.S. Government. There is so much that is on paper right now that I think is a huge problem, and it is preventing us from serving our customers, citizens.

I think this is important because the way that we value our electronic systems and IT is primarily data. Data is what we use to measure. We understand how we are doing. We are providing value with data. When that data is locked into paper, in warehouses—and I have been to a few of those warehouses that we own as the Federal Government—that is data and value that is locked away from us to use.

When I was CIO at the Department of Energy, we spent a good amount of time, and it started on the front end, moving to digitizing documents, and that was both to provide better service, but it was also to free up some of that value of data. That data could help us drive our management better, it could help us serve better, not only citizens but everyone doing the mission in the Department, and that is really what we are supposed to be there for.

I want to really quickly talk, and people have already hit, I think, on these two subjects. Most of the time in IT we talk about people and we talk about process. Renee already, I think, mentioned very well some of the people problems that we have in government. I can tell you that our human capital system needs dramatic improvement. We simply cannot compete. We cannot even get access to some of the people that we need to recruit in government if we are going to move to the cloud. If we are going to move to managed services, those are new skill sets. There is a place for retraining our employees, but right now we are not doing that very well either. I think it is important to continue to look at that issue of human capital.

I can tell you, as a CIO, I had a number of authorities on paper to be able to go and hire new people, to use more creative ways of hiring. It was rare that I was ever able to use those. I would walk into meetings with people, having printed out documents from the OPM website stating my authorities to be able to hire, and yet was unable to use them. That is a critical failure that has to change, and it is a communication issue, and it is an oversight issue.

I do also want to very quickly mention, with gratitude, that I know Congress recently allocated more money for the U.S. Digital Service (USDS) and other groups. I think that is important. The U.S. Digital Service is an opportunity to bring in some very experienced people from digital backgrounds who want to serve the U.S. Government, and that is great. My encouragement for them is that they focus on sustainable, commercial solutions. Those are the things that will last. Those are the things that the current CIOs are actually going to be able to sustain with the workforce that we have. I think that is important.

I also want to quickly mention contractors. We cannot discuss the people issue in government without talking about contractors.

In most departments, the number of contractors in IT typically outnumbers the Feds by 3 or 4 to 1, or more, and we need to understand that if we are going to deal with that problem.

I very quickly, then, want to jump into a couple of things I know we will talk about further. We already mentioned TMF. I am a strong proponent of TMF. TMF is not about the money, although we certainly appreciate the billion dollars that have gone to TMF that will radically change that program. It is about the process of actually getting those grants, what you have to go through. It changes the way that we should be managing IT in government. I think TMF is important.

I cannot let the opportunity pass without mentioning, I know that there have been some conversations about waiving the repayment. I would encourage that to be given some thought. I am supportive of it, as long as the process is followed. The TMF process is as important as the money, because it means we are counting our costs, we are looking for savings, and we are managing things in the way we would expect anybody to manage our own money. I think that is critically important in all those conversations, and to make sure that the TMF money that has gone over goes to the TMF process, that it goes through the committee and the board that is there, and goes through proper oversight. I think that is critical.

With that I will conclude my remarks and look forward to your questions.

Senator HASSAN. Thank you to all of you for your excellent testimony. We are now going to go to rounds of questions from Members of the Subcommittee. I will start. Each round will be 7 minutes, and do try to be mindful of Senators trying to move to other witnesses as you give your answers, please.

Why don't I start with a question to Mr. Walsh. I would like to start by identifying the costs and consequences of relying on legacy IT. We have established what we mean by legacy IT, namely systems no longer supported by industry vendors or custom systems that are difficult to manage and adapt over time. However, what is more difficult to define are the costs, both quantitative and qualitative, that continued reliance on legacy IT produces.

Mr. Walsh, how does GAO determine costs associated with legacy systems, and how can agencies improve their identification and reporting of these costs?

Mr. WALSH. Identifying costs associated with legacy systems is more difficult than one might think. As Mr. Everett noted, the fax machines do not show up on a spreadsheet. They are hard to figure out. You can look at our inventory of IT systems, but we finished getting a complete inventory of our software licenses for each of the major CFO Act agencies this past year. We still need to work on getting better inventories of what IT we have out there before we can fully capture the cost.

There is a nascent effort underway called technology business management (TBM), which would closely tie accounting systems to our IT oversight and management systems, which would help allow us to better track where the money is going. But to answer your question, there is no good way right now to identify all of the legacy IT in government.

Senator HASSAN. I want to follow up with that, because as I mentioned in my opening statement, roughly one-third of total Federal spending on IT went toward legacy systems in 2020, but many experts believe that that number does not capture the whole picture.

Mr. Walsh, what are we leaving out of our calculations on legacy IT costs? How can we better factor in qualitative or performance costs associated with legacy IT systems?

Mr. WALSH. One of the biggest issues with the dollar amount is the $90 billion that this is all predicated upon is dramatically understated. That $90 billion does not include weapons systems, satellites, or supercomputers. There is a lot of IT in the government that one might think, “Hey, that is certainly IT,” that actually is not included in that number.

Getting all of that IT accounted for is the first big step. Once it is accounted for, having that accounting system tie into our technology management would help us get better to see if the money is going for specific hardware or software usages. But this is not a silver bullet, easy fix. This is going to take time.

Senator HASSAN. Thank you, and I will follow up with you on that probably in another round of questions.

But let me move on to Ms. Coleman right now. The American people pay the price of failing to modernize legacy IT systems. The U.S. Government ranks among the lowest industries in customer satisfaction.

Over the past year, in particular, my office has received hundreds of messages from constituents struggling to access passports and visas, unemployment benefits, economic stimulus payments, benefits information from the Department of Veterans Affairs (VA), and information on filing taxes. We have also heard from Federal employees like those at the National Passport Center in Portsmouth, New Hampshire, who want to respond to the needs of the American people but simply cannot do it because of their limited IT capabilities.

Much of this is due to the antiquated paper-based systems that cannot support 21st century agency missions or respond to changing requirements during a pandemic. Ms. Coleman, how important is it for agencies to recognize that failing to modernize means failing to serve the American people?

Ms. COLEMAN. Thank you, Chair Hassan. I think it is a vital issue, because, as you point out, we interact with the government on really critical services that we count on, and if those services are not delivered effectively there is a cost. There is a cost in terms of employee productivity and in terms of our time as citizens and as the public. There is also a public trust at stake. There is a confidence in the ability of government to deliver what we are anticipating as taxpayers and as citizens. I think that public trust is one of the key costs.

I think that it starts from the way government has been designed and operated. Our systems reflect the way the government is set up, sort of from the inside out, with the programs designed around different siloed functions. As we interact with government we do not think that way, but we are forced to navigate the complexity of that bureaucracy. I think one criterion to change this is to start to think from the outside in, from the point of view of the customer or the resident that is navigating that process.

There are very encouraging success stories. For example, U.S. Department of Agriculture (USDA) has created farmers.gov, which is a portal for all services delivered by the U.S. Department of Agriculture, so you do not have to navigate separate programs for crop loans or disaster insurance or conservation research. All of these things have been integrated and delivered in a holistic way, and it offers an example for others to be mindful of.

Senator HASSAN. Thank you.

Let me follow up. Mr. Walsh, can you describe agency efforts to prioritize customer experience through IT modernization? Ms. Coleman mentioned one at the Department of Agriculture, but I think the Department of Education also comes to mind as a leader that has used IT modernization to improve customer service and mission readiness.

Mr. WALSH. That is correct. The Department of Education has actually modernized all of its data centers. It is now almost entirely in the cloud, and to its credit it is moving to get away from legacy. That is not say that their modernization journey is done, but they are a leader in that area.

Senator HASSAN. Thank you. I am going to get through one more question. Some have argued, Mr. Walsh, that maintaining legacy systems, especially customer-built systems that rely on antiquated coding languages and lack connectivity to other agency systems are insulated from cyber threats and do not need to be modernized because they pose little risk.

Mr. Walsh, do you agree with this argument, and if not, what would be a better risk management strategy than simply maintaining legacy IT systems in perpetuity?

Mr. WALSH. Legacy systems represent a security risk. They are not good at meeting our mission needs. They cost more to maintain because a lot of times the people who can maintain them are retired or, in some cases, deceased. They increase our cost every year. I do not think that security through obscurity or hoping that the bad guys do not know the system code, is a good approach.

Senator HASSAN. Thank you. Ms. Wynn and Mr. Everett, the agencies you have worked for both handle extremely sensitive information that may be stored on legacy systems. How did you balance the need for modernizing legacy IT systems with mitigating risks inherent to storing sensitive information? Why don't we start with you, Mr. Everett, and then quickly on to Ms. Coleman?

Mr. EVERETT. I will quickly say that was an enormous challenge for us, as Kevin already said. One of the issues you have with legacy systems is you cannot put modern protections on them—multifactor authentications, encryption. The secret of those systems is to even work today they often have to have a number of these little enabling things we call system accounts or administrative accounts. When you are an administrative account you know that is exactly what a bad guy wants to use, because once they have it they can use it to access and do other things in your system.

That is one of the dirty secrets of those older legacy things. They are not protected more because people do not know them, they are, in fact, enabled by a bunch of other things, and pretty soon it is a Rube Goldberg apparatus.

Security is also about resilience. One of the reasons your constituents cannot get on those is because they fail all the time. Why? Because they are old and they fall apart and nobody knows how to fix them. That, in and of itself, is a security risk, because everything else in the system has to adapt around that, which causes you to make all sorts of other security compromises to keep it going.

Senator HASSAN. Thank you. Ms. Coleman, very quickly on that issue, and then we are going to move to other Senators.

Ms. COLEMAN. Thank you. The point is well taken, and one of the key issues with securing data, many times it is good cyber hygiene. Estimates are that well over 50 percent of all incidents are due to basic good cyber hygiene. With modern platforms you are really taking advantage of best-in-class security and a partner who can assist you with that. But really, ultimately, the government needs to start with basics and maintain good protocols.

Senator HASSAN. Thank you very much. I thank you all for your answers. Now we are going to turn to other Senators, and first up is Senator Rosen, who has been very patient and is very knowledgeable on this issue. Senator Rosen, you are recognized for 7 minutes.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chair Hassan, for organizing this important meeting. Chair Hassan, you have done so much work on the issue of Federal IT management. It is critically important to serving our taxpayers, to saving us money, to delivering services, as well as boosting the morale and effectiveness of our Federal agency workers. I really appreciate everything that you have done.

Of course, a common theme that has emerged from all four of our witnesses is the importance of the Federal workforce in implementing IT modernization at our Federal agencies. I have to admit that I actually wrote COBOL legacy IT systems in the 1980s and the 1990s, and so I intimately know exactly what you are talking about. It makes me feel a little old, but we do need to move forward on this.

I have been working with my colleagues on this Committee and across the Senate to address the nation's shortage of these kinds of technical workers and cybersecurity workers, and Federal public service positions. They really should be attractive to those folks who want to work in tech.

I joined Chairman Peters and Senator Hoeven in reintroducing the Federal Rotational Cyber Workforce Program Act. It is going to provide opportunities for our civilian cybersecurity employees to rotate amongst various Federal agencies. It expands their experience, expands their professional networks, and expands their opportunities to serve the country.

Last week I introduced a bipartisan bill with Senator Blackburn to allow DHS and DOD to establish a Civilian Cybersecurity Reserve Pilot Program. It would call on former military and civilian cybersecurity employees and others for temporary assignments in the government. I think this can serve as a model for other agencies.

Mr. Walsh, in the course of GAO's reporting on your IT modernization efforts, have you identified agencies that have done particularly well in recruiting and retaining these types of employees? How do we export those best practices? If you have not, does OMB and OPM play a role, and how do you see that role?

Mr. WALSH. We have not done specific work—I should say I am not aware of specific work in that regard on hiring cyber employees. Now I do know that, as Mr. Everett mentioned earlier, the U.S. Digital Service as well as 18F serve as ways to get private sector talent into the government. I do not know if they are as quick as your proposed legislation is considering. But having that venue for external talent to come into the government and share ideas and propagate those ideas is very important.

CIOs also do have additional authorities that they can use to hire and bring in folks from the outside, but Mr. Everett earlier identified issues with executing some of those authorities. GAO has not done specific work in that regard, but I am eager to work with your staff on that.

Senator ROSEN. Thank you. I appreciate it.

Ms. Wynn, in your testimony, you mentioned there needs to be civil servants who are working on every Federal IT project and that those workers need to be reskilled. You said that early efforts to reskill existing Federal employees have been successful. Can you elaborate on what type of reskilling was the most successful, and what areas we need to still reskill in, so we might direct our efforts in creating workforce and training in that workforce pipeline?

Ms. WYNN. Thank you for that one. The Office of Management and Budget, through the Federal CIO Council, through their Workforce Subcommittee, established a reskilling institution or program. A lot of Federal civil servants applied to this program. They took an aptitude test for cybersecurity, and from there the top folks were taken, and yet they still had to cut the number of participation to a low number, because it was our first-ever endeavor. Those folks went through some training programs and proved themselves to be very capable cybersecurity professionals, and then went on to seek future employment, still within the Federal Government, but in this case a job change.

The bottom line is Federal Government workforce is talented. When we show them the way and give them the time and the support to get reskilled, we can take their talent and use them in other places, especially in cybersecurity.

Senator ROSEN. Thank you. I look forward to working on that.

I would like to move on now, and again, Ms. Wynn, I want to talk to you about IT modernization and support to national security. Given your background at the Department of Energy, which houses the Nevada National Security Site, located not too far from Las Vegas, it is facilities that are critical to our security. Can you comment on why modernizing the Federal Government's IT and cybersecurity infrastructure is critical to our national security and safety. Particularly as it relates maybe even to our nuclear stockpile, how do we move forward, create more nimble, secure platforms and firewalls to protect our national interests?

Mr. EVERETT. I think——

Ms. WYNN. Senator Rosen, why don't I get started and then Max Everett might be able to——

Senator ROSEN. Perfect. I am going to him after you.

Ms. WYNN. That is great. I will get it started because critical infrastructure, right now the space, and flying in space in satellites are being thought about as critical infrastructure because we rely on them for logistics. Moving anything around this globe requires satellites, navigation, if you expect it to get there and avoid significant weather events. That type of security is very challenging.

You need the cooperation of a number of parties, including all those that operate the infrastructure. You have the electric grid, you have the water infrastructure, and in this instance I mentioned space, and those folks have to get together and first and foremost recognize that there are real threats in space, space needs to be acknowledged as an element of the business practice as well as part of critical infrastructure. In that case, work as a team to put into place and take steps toward securing it better.

At NASA we were beginning to do that, by taking a look at our critical satellites and then trying to figure out the best way to secure them in this current environment. As noted previously, we cannot bring back our older satellites and give them a new operating system, but we can do things here on terra firma, as I call it, to secure them better, and then we have to apply good neighbor policies, because we fly in the same place as other countries, as well as the Department of Defense, and private sector. Again, working together to protect our critical infrastructure is what is needed to get the job done.

Senator ROSEN. Thank you. Mr. Everett, I know my time is up, but if you could be kind of quick about it, that would be fantastic.

Senator HASSAN. I will add that a number of Members have conflicts and are not going to be able to come, so Senator, if you want to take a couple of more minutes and the witness too, that is fine.

Senator ROSEN. OK. Mr. Everett, then please. Please elaborate.

Mr. EVERETT. I will. Thank you. You are right. The Department of Energy, one of the great challenges at the Department is the breadth of its mission. Certainly some of us know that they have a nuclear mission for protecting, building, and designing the nuclear stockpile. But that mission stretches all the way down to fundamental science that is conducted with scientists around the planet. We have what are called user facilities that are used by the top scientists around the world to do collaborative scientific basic research that not only helps the United States, certainly, but really helps the entire planet. One could argue it is almost a diplomatic role that we play in science because of that. With those very divergent missions it adds an extra layer of challenge for the Department of Energy.

I would say there are three sort of focus areas that we try to work on, that we think are the most important for that. One of them is simple visibility. Visibility is about being able to see and understand, as we talked about, what do you have? What actual systems do you have? What legacy systems do you have? Who is on your network? That is a critical element, and it is one we have not done very well as the Federal Government.

I think some of you are already aware, and it has been discussed over the last few months with the cyber incidents we have had, there have been some significant challenges with the EINSTEIN program that needs to really be very carefully re-looked at. I would tell you in our own department that was a challenge of basic reporting and visibility of what was going on across our whole footprint.

The second part of that is risk management, and this was where we put a lot of our focus. When you have a large enterprise like NASA, Department of Energy, GSA, and you have divergent levels of risk, we will never have enough resources. When I was CIO, I was always glad to come and ask Congress for more money, but you only have a certain amount of resources to go around. Risk management is looking at what are your top risks, what are your most important things, and they get the first dollar, and you find that balance.

That is what risk management is, and it takes real thought, and it takes effort, and you need to document and discuss and be able to defend your efforts. We spent a significant amount of time because it is critically important.

The third element I would talk about, and it starts to go to what we are talking about here today with legacy and modernization, is moving to new models. Some of you may have heard the term "zero trust networks." Fundamentally, you cannot use zero trust networks with legacy, because they require some new tools to be able to better manage what is on your network and make sure that those things can essentially tell other things on the system that they are allowed to be there and do what they are doing. That is very difficult to plug into a 20-year-old system. These newer models like that simply will not work in those legacy environments. They have to be updated to do it.

Another area I would mention here is FedRAMP. FedRAMP has been around. It was started for a good purpose. I still think it can serve a valuable purpose. But I would tell you FedRAMP is far too slow. I do not know of any vendor that I talked to in my time at CIO or now who does not complain about the timeline for FedRAMP.

What that means is probably FedRAMP needs some more resources, because what FedRAMP does is it does the baseline security work one time, so it is a shared service. It is doing that one time for everybody so that you can then start to bring more innovative solutions to market more quickly in the Federal Government.

We are missing out on opportunities. I recently talked to a venture capital person. He told me, for some small and mid-sized companies with unique new services, primarily software as a service, that it was taking them four to five people at $1 million and a year to go through FedRAMP. For most of these startups who are coming up with new, innovative, new things to do, that is not sustainable, and we are going to miss out on those opportunities if we cannot improve that process.

Senator ROSEN. Thank you. I have a closing statement, but I am glad to ask other questions. But one thing I know for sure is that good code means speed. Good code means ease of use and data capture for the end user. Good code means the better the data capture for analytics for our future. It saves us time, it saves us money, it improves outcomes, and it helps us plan for the future.

By modernizing these systems, by having safe, secure systems, by capturing more data in consistent ways, we are able to predict, plan, and protect ourselves, and we have to do that.

Chair Hassan, I am glad to continue to talk about this. I am not sure if someone else is in the room, but you tell me.

Senator HASSAN. Thank you, Senator Rosen. I think right now it is just you and me, and I have another round of questions. But if you have a couple more why don't you go ahead and then I can finish up with my round.

Senator ROSEN. You know what? I am going to hand over to SASC, where I think I am finally up over there. I appreciate everyone being here. I appreciate what you do, and I sincerely hope that we can try to, I guess even one system at time, continue to get off those legacy systems onto something that is newer, more nimble, and allows us better data capture so we can continue to take care of everything that we need to. Thank you.

Senator HASSAN. Thank you, Senator. Now I will turn to a second round of questions, and I appreciate the testimony you all have provided so far. I am going to start with this question for Ms. Wynn.

I have advocated for a biennial budgeting cycle where Congress would determine and appropriate the budget in one year and then year two can be spent on doing effective oversight to inform future spending. The current one-year cycle often leads to hasty decision-making and neglects capital investments that take several years to implement, including IT modernization projects designed to move away from legacy IT systems.

Ms. Wynn, how difficult is it to manage IT modernization around the one-year budgeting and appropriations cycle, and how did you work within this cycle to achieve your goals? What would you have done differently if there was a biennial budgeting process?

Ms. WYNN. Thank you, Chair Hassan, for the question. One of the things that I have found, first, is sort of annual appropriation, first thing you need to know is every time you cross a fiscal year with a project, and most IT projects cross a fiscal year, you add more risk to your plan, and that is because from year to year you face the potential loss of funding or the loss of people.

Now you have disrupted your project, and now you have most likely extended when you are going to get that project done. That extension, if it goes on too long, means you are potentially using software that will no longer be considered modern or available, or could reach end of life by the time you use or get that system back in operation after it has been modernized.

What I would do is, and probably what most CIOs would do, is I would take my total budget and I would create a reserve, and that way the reserve would be used to make sure that the most critical, the highest-risk projects would get funding, going into the secondary years of their project. That way I knew that they could be able to continue. If I did not do that, I would run the risk of work stoppage, and then I could lose the talent of my staff, of staff from other mission areas or mission support, or I could even lose contractor staff, and that would, again, start to slow down and add more risk to your project.

If I had a second year added to it by a biennial, I would be able to take the projects and draw a timeline of people and dollars, and make sure that they were spent according to it, and hold people accountable to a two-year increment. This would reduce the risk in a complex IT project, because you did not have to worry about funding every few months, because by the time you get appropriations finished and you get the new authority money, several months in the fiscal year have gone by, you could actually plan about 18 months and be assured of those resources, therefore reducing the risk of managing a complex IT project and you could deliver that project a lot faster because you would take out that funding issue, or convert the funding issue to an 18-month issue instead of a 9-month issue. That would be hugely beneficial and a great gift to CIOs and program and project managers around the country.

Senator HASSAN. Thank you. Ms. Coleman, at GSA you worked to develop FedRAMP and streamline agency IT acquisitions in coordination with industry partners. You now work for one of those industry partners that is trying to help the Federal Government modernize its systems. What is the impact that the one-year budgeting and appropriations cycle has on industry and its ability to support IT modernization efforts?

Ms. COLEMAN. Thank you, Chair. I agree with everything that Renee said about the ability to plan over long-time horizons. It is almost even not a nine-month planning horizon with the annual cycle we have now, because of the frequency of continuing resolutions (CR), which create even greater uncertainty about available funding and disruption of resources. That alone is a complication.

One thing I would like to suggest as a companion idea to a two-year planning and budgeting cycle, which I think is a much needed and helpful measure, is greater use of agile DevOps tactics to break modernization projects into short sprints that deliver short and relatively quick intermediate results, so that there can be fine-tuning and transparency and oversight throughout the process. Any project that is intended to deliver results in 2 or 3 years is going to be out of date by the time results are delivered. We need to be thinking about very short, rapid cycles to deliver results, and the accompanying oversight and funding to go with it.

Working capital funds of previous legislation have been very helpful. We used that with great success at GSA. We also implemented a zero-based budget so we could see where our incumbent costs were and understand where we needed to place our dollars for modernization priorities.

Senator HASSAN. Thank you. That brings me to another set of questions, and I am going to start with Mr. Walsh, concerning agency modernization plans.

Currently, agencies are not required to develop or publish IT modernization plans. While many agencies have developed plans, some of these plans fail to establish concrete timelines, cost estimates, and goals. GAO recognizes that having an IT modernization plan in place is essential to reducing reliance on legacy IT systems.

What makes these plans such a valuable tool, and how can agencies better leverage them to meet their goals and manage their resources?

Mr. WALSH. Having these plans is valuable, to get agencies thinking about it. In agencies that do not have a documented plan, we are not sure what kind of resources they are going to be able to throw, what kind of timeframes, even the scope of the project. Having some idea of what needs to be done is kind of the most fundamental step, and in our 2019 report, it was very disheartening to see that three of the agencies did not have a plan, an additional five had some aspects of a plan, and only two really had a firm idea of what needed to be done.

It is critical because modernizing legacy systems is critical to the government's security and privacy and how well we serve our citizens. Getting our agencies to be thinking about modernization is the first step.

Senator HASSAN. Thank you for that. One other key element that modernization plans, when they do exist, often omit is how the agency plans to manage costs arising from maintaining a legacy system while they are also implementing a modern system.

Let me turn to Mr. Everett now. In your time as the Chief Information Officer at the Department of Energy, how did you manage the competing investment needs between existing systems and new systems? How might agencies leverage modernization plans and existing resources to offset what is essentially the cost of the overlap?

Mr. EVERETT. I would tell you much of my experience was, to be very frank, robbing Peter to pay Paul. In most cases, to do those modernizations, you are going to have to take money from somewhere. I think to Kevin's good point that you already brought up, without a modernization plan you cannot have the planning. I was, frankly, somewhat fortunate as a CIO. We had some monies that were multi-year monies, that gave some level of help to us in being able to plan, but I know many of my peers had only single-year money, which was a great challenge. I think your discussion of a biennial is certainly helpful.

The other one I would bring up, certainly, is things like TMF, and within the MGT Act, the idea of Working Capital Funds. I know that there is long-held concern about Working Capital Funds turning into slush funds and things of that nature. I think that simply means they need to have the appropriate oversight. But they would allow that level of longer-term planning.

Listen, anybody can put out a modernization plan, but if they do not have the money to back it up or the people to execute on it, it is not going to work anyway.

I will also say I think what Ms. Coleman said is absolutely correct. Kevin could probably sit for hours and tell us stories of programs that have been run in the government for multiple years, these large projects, millions, if not billions, of dollars wasted, that did not ever come to a finish line, or even worse, came to a finish line, and were probably even reported as being on time and schedule, and yet provided no actual value to citizens, to anyone.

Breaking things up, that agile method of breaking things up and doing it in those smaller chunks is appropriate. There are very few systems that we should be building in government anyway. We should mostly be using commercial. Where we do need to build those—and certainly Energy, NASA, and other places have those use cases—they should be done in an agile way where you can have some oversight, make sure they are delivering value on an iterative basis, so that you do not have to plunge hundreds of millions of capital expense into something, only to come to the end of the road and the money is all gone. I think that has happened far too often.

It always a challenge, again, for us. We had a little more flexibility, but even I had to have a lot of conversations. Renee made the right point—you often simply had to build a reserve, and that reserve was usually coming from other things you would have liked to have done that were customer service-oriented or those kind of things. It is a real trap, and it builds what we call technical debt. It is not the monetary debt. It is all the things we cannot do that are a part of that.

Senator HASSAN. I thank you for that, and I am going to take advantage of a rare moment in the Senate, because we have a little bit more time and you are such an excellent panel. I have two or three more questions, so bear with me. But I think we are learning a lot here.

I want to turn now to the issue of the authority of Chief information officers. I want to start with a question to you, Ms. Wynn. The Federal Information Technology Acquisition Reform Act expanded the responsibilities of agency Chief information officers and requires their input on IT acquisitions to realize cost savings and to manage IT inventories. However, despite the good intentions of this law, GAO has found that Chief information officers do not receive adequate deference on IT planning, budgeting, and management.

Ms. Wynn, can you speak to your own experience as a Chief Information Officer, both at the Environmental Protection Agency and at NASA, and how you worked to get institutional buy-in from agency leaders to advance your IT modernization efforts?

Ms. WYNN. Chair Hassan, I would begin by saying never let a crisis go to waste, when it came to exercising the authority and making culture changes and process changes within a Federal agency.

My first example comes when I first arrived at NASA and noticed that, as Max earlier said, you need to know who and what is on your network, and NASA did not have that ability to look at the network associated, used across the globe, and it is relied upon for the NASA flying assets, satellites. At that point I could easily go to the leadership and say, “How do you know you don’t have problems? How do you know you have problems?”

We began the process of rolling on the Continuous Diagnostic and Mitigation Program. With that transparency, with that visibility, we got to see what was on our network, and there was a lot of inappropriate software and activity on the network. Then I used that data to share with agency leadership, to say, “I do not think it is OK for us to have this type of software on NASA’s network.”

From there I would build, with this visibility that we got, tell stories back to folks, and turn it around to say, “This is not acceptable for a public agency,” and use the pride that my colleagues had about working for NASA to really propel us forward. With each fiscal year we got better at working as a team by gaining that visibility.

Then what we did is when I mentioned the business services assessment, and also the follow-on to the business services assessment, when NASA said functional areas such as the CIO needed to have control over the appropriate IT budgets. This was also true for procurement. My colleague in the procurement office recognized that IT needed to be procured better, and stood up an IT division while I was still there, and we worked very closely with her to set that up. The establishment of that IT division meant that all IT purchases for NASA would have to go through that division, and that I or my team had significant influence over that acquisition process.

That took about 18 months to get set up. It got going in full swing after I left NASA. But by having a crisis, by having visibility, and by forming partnerships, NASA was able to continually iterate in order to give the greater authority over to the CIO, gave IT procurement greater visibility into what NASA was buying, and with that visibility and with that partnership, each year that I was there at NASA we were saving about $50 million a year on software purchases alone.

Real differences can be made through partnership, and I will close with the same thing I started—with never let a good crisis go to waste. Just stand in someone's office, make a friend, and get going on fixing the crisis and changing the processes that might have created that crisis.

Senator HASSAN. Thank you for that answer. There is a lot for us to learn from that and from your experience and your good work.

Chief information officers spend an average of 2 years or less in their position, so I am concerned that this short tenure provides very little time for CIOs to be effective or establish fiscally responsible practices.

Ms. Coleman, you spent 12 years at the General Services Administration. Do you think that your ability to stay with the agency for that long contributed to your success as a CIO, and how so?

Ms. COLEMAN. Absolutely. It allowed me to really understand the culture of the agency, and to the point Renee made, to build relationships and partnerships with senior leaders, because modernization is a team sport. It is important that CIOs have adequate authority. But it is also important that top leadership understand the role that they play in supporting transformation. To the point you made earlier about the need for modernization plans, it should start at the top and be a priority, even of the Secretary or the administrator of the agency, and at the political appointee level.

By having a long tenure at GSA, and in the role of CIO, I was able to understand that, and be able to use the tailwinds provided at GSA. It is an agency that provides business services to other agencies, so they take pride in understanding technologies to be a good supplier and partner with other agencies. That gave us momentum with moving to the cloud, because we were able to tap into the culture of what the agency is good at, and the DNA to support it across all lines of authority. That alignment, not only with leadership but also with my peer, the CFOs, the head of HR, and so forth gave us the unity of leadership to make real progress.

Senator HASSAN. Thank you. I am going to now turn to Mr. Everett, because you had a slightly different experience at Energy, because you had a brief tenure at the Department of Energy, but you were also able to be extremely effective. What do you recommend that current and future CIOs do to be most effective from their very first day, and then forward, at an agency?

Mr. EVERETT. I think there are some tremendous challenges on that, and part of this gets into the conversation of political versus career CIOs.

Senator HASSAN. Yes.

Mr. EVERETT. There is a tradeoff. I absolutely agree, the longevity is critical, because they can understand the mission. The political ones typically are going to have more access to senior leadership, so there is a bit of a balancing act there.

What I would tell you is part of the reason I was able to be effective is I had been in Federal Government before. I knew the ropes. I knew what I was getting into. I routinely tell people, as just sort of shorthand, if you are new to Federal Government, it is going to take you a year to know which way is up. If you are coming, no matter how smart you are, from the private sector, you are going to have to go through a whole year, just to know which way is up, all the differences that you have there.

Because of the nature of the timing—again, going back to budgets—because of the timing of budget, you are going to go 2 years before you are working with your own budget that you had any input into. When I walked in, in 2017, my initials were at a budget formulation that had already been submitted to OMB. By the time that goes clinking around through the entire process of OMB, back to the Hill, it is October, a year and a half later. That is really challenging.

I have talked to people from both parties who have been very involved in trying to recruit innovative leaders to come in as CIOs, and you will find ones that are willing to give up the money. They will divest their stock. They will take a salary hit. They will move their family. They are willing to serve our country, and then they find out, it is going to be 2 years before you can actually make an impact? That is a killer, because their whole reason of doing such a thing is to make an impact. If they are politically appointed, they know they have a shelf life, and that is a really hard sale. It has made it really challenging.

We have great career folks, as well, that have done really good jobs as CIOs, without question, and so my emphasis is definitely there, of giving them more authorities. I would love to get some of those outside CIOs, regardless of political affiliation, because, thankfully, IT is the last nonpartisan issue in town.

I would love to have those people. I would love to have those innovators. But we do have to have the structure so that they feel it is worth the sacrifice to come in and bring that experience and innovation that they have from the private sector. It is critical. In the meantime, we have plenty of great careers, CIOs and deputies, out there. Giving them the tools. FITARA is an important tool, but you have to know how to use it.

I have been in probably the three most spread-out agencies—DOE, I spent time at Commerce, and at DHS. I would describe them, at best, as a feudal system, if not a mob family, and you have to be able to pick your fights. I have seen CIOs who have gotten run over because they did not use FITARA appropriately.

Renee made a great point. Procurement was a great ally to me in the process. I would tell people, walking in, your procurement officer is going to be a great help. I will pick a fight and say, we need more support versus the CFOs. CFOs typically are Senate confirmed.

Senator HASSAN. Yes.

Mr. EVERETT. Only one CIO, VA, is Senate confirmed. In the pecking order of this town, it is very difficult for CIOs going up against a Senate-confirmed CFO. You can make a great relationship with them, but at the end of the day, they are higher in that pecking order, and that is a challenge for many CIOs, because you are not sort of quite at the same level.

Senator HASSAN. Thank you. I am going to turn to one other topic before I ask you a wrap-up question, and it is something all of you have mentioned, but I want to focus in on it a little bit. I want to start with Mr. Everett.

As part of the American Rescue Plan, the Technology Modernization Fund received $1 billion to loan to agencies in order to modernize IT systems. Although we do not see the impact of these funds for years to come, this is a really major step forward to reduce reliance on legacy IT, and I hope that the fund prioritizes agency plans to replace the legacy IT systems that we have discussed today.

Mr. Everett, as a CIO who successfully leveraged the Technology Modernization Fund to move away from legacy IT systems, how should agencies utilize the fund to ensure that they not only have the resources and infrastructure to support IT modernization, but also ensure that the systems they propose actually reduce reliance on legacy IT while contributing to better security and customer service?

Mr. EVERETT. The first thing they should do is have the courage to actually go apply for those. I think if you go look, I believe it is still only five agencies that have actually received TMF funds. I spent a lot of time browbeating people, and I know people, they were simply afraid of the oversight, afraid of the visibility. They were also afraid of the repayment, which is why I think that has to be looked at.

But a lot of them—listen, from my team, the culture chain was important. I had members of my team, my career team, come back and tell me they enjoyed the process. They went through a process that is similar to anybody who has ever worked in private sector. You can go right now to the website, the TMF website, and go through the spreadsheets, and see the level of detail that you were asked about your current cost basis and your future cost basis. That is how everybody in the private sector runs their IT. That is exactly how we should. We should know all of our costs, across the board. We should be able to project them out over years. That is what any mature organization would do, and that is a huge value of the TMF, and you need your people to do that.

Literally, I do not care if you do not turn it in. Everyone should go do one of those today. Everybody in government. I think part of it is being brave enough to step forward and go ahead and do it, know that there is going to be that challenge. There is oversight to it. The board checks in on you, so you do not get a giant check.

Senator HASSAN. Right.

Mr. EVERETT. There is a process to it, and that is critically important. I would urge all of you—I have been in this town 20 years. When Congress gave $1 billion to a program that most people kind of do not understand, I know for a fact, in this town, there are people eyeballing that money, who want to cut the line and avoid the process. I would strongly urge you to make sure that your oversight does not allow that to happen. That process has to be followed. Now, it can go to all sorts of things, and so to your point, those legacy systems are probably, arguably, the easiest ones to show, in many cases, where you can get value and return on the investment, and they are great.

But I will also mention—and this is where some of those waivers need to be looked at—there are so many customer-facing systems, it is very hard to document the cost savings there. The customer service, we can talk about all day long. You can see it with your eyes. But it may be harder to show the cost savings on that system, and that is where I think we do need to look at some ability to defer away costs, as long as the process is followed.

I am such a proponent, as you can tell, of TMF, because that process leads us to how we should manage things. It should not simply be giving things out to a most favored program.

Senator HASSAN. Right.

Mr. EVERETT. We have done that too often, and that is a disaster. Making people go through the process is just so critical, and I think any CIO coming in right now, it is a great test of your team. Ask them to go find you—I would challenge any new CIO——

Senator HASSAN. Yes.

Mr. EVERETT [continuing]. Tell your team to find one program or system that needs to be modernized, and make them fill the form out and take a look at it, and you should be able to tell right there, do they know their costs, do they know their systems, do they understand how to project that budget? If they do not, get help.

Listen, there are some great groups in town, some truly private sector associations, that will come in, free of charge, and come help you with your acquisition and your budget process, and they are not trying to sell you anything.

Senator HASSAN. Yes.

Mr. EVERETT. As well, Kevin mentioned TBM. Another great process you can go through to understand, in a very modern way, how your costs should be managed. There is help out there for anybody who is looking for it in the Federal Government right now, if they are willing to reach out.

Senator HASSAN. Thank you. I am going to turn to Ms. Coleman, too, about Working Capital Funds. I will also note that one of the issues you raised is how we go about qualifying and quantifying customer service value, right? Because, obviously, for taxpayers, our goal should be to make the interface with the Federal Government as customer friendly as possible, since taxpayers are footing the bill here. Trying to figure out a way to really assess value there, I think is really important.

Ms. Coleman, Working Capital Funds are another mechanism that agencies can use to support their IT modernization priorities, outside of the one-year budgeting and appropriations cycle. While some agencies have the authority to establish these funds under the Modernizing Government Technology Act, some agencies were not given the authority, which is a technical error that I hope to address in future legislation.

Ms. Coleman, the General Services Administration effectively uses Working Capital Funds and fees generated from its governmentwide services to fund its mission. Can you describe how GSA uses savings produced from modernization projects to keep the Working Capital Fund going?

Ms. COLEMAN. Yes. Thank you. One of the keys is to take a portfolio approach, and I completely agree with what Max said earlier about the Working Capital Funds. Modernization, in and of itself, will incur cost and complexity when viewed in isolation. One way to counterbalance that is to look across all systems and all investments, and to be able to do puts and takes in a portfolio-based approach. If you have a Working Capital Fund, you can know your money and you can time the modernization according to your risk management and according to your most critical systems first, or the ones that deliver the greatest impact.

As it pertains to customer service, that is a qualitative measure, not so much quantitative measure.

Senator HASSAN. Yes.

Ms. COLEMAN. But the ability to stay up to date with platforms that are maintained by the vendor, rather than having to continually invest with agency resources for these big upgrades every 2 or 3 years, provides cost savings along the way as well.

Senator HASSAN. Thank you. Mr. Walsh, from GAO's perspective, what are the advantages or disadvantages of relying on the Technology Modernization Fund, or Working Capital Funds, to resource IT modernization rather than requesting funding through the annual budget requests?

Mr. WALSH. As the other witnesses have noted, the TMF allows agencies to kind of shortcut the budget cycle. Now, it is still a loan. It is not a free gift to go out and spend willy nilly. You go through the application process. I will also note that the process, as described, going through TMF that Max talked about, is very similar to having the modernization plans that we described. You have to have some idea of the work to be done, the timelines, and a plan to turn off the old system.

The disadvantage to the TMF is that it is linked to spending and cost savings. There are times where we need to modernize systems, and they will not save money.

The OPM breach that we talked about earlier——

Senator HASSAN. Yes.

Mr. WALSH [continuing]. The government had the choice to modernize those networks and systems to allow the data to be encrypted when it was at rest. It was a tradeoff. I am sure if OPM wanted to go back in time and had that decision to make, they would absolutely spend the money to modernize that. But they would not save any money by doing that modernization.

Modernization is not about cost savings. It is about better services to our citizens, privacy, security. Cost savings can be a part of it, but there is a lot more to this decision than just the money.

Senator HASSAN. Thank you. That concludes the rounds of questions I had. I am going to ask you all one wrap-up question, and just double-check with staff—we are good on other Senators, right? OK.

First of all, all four of you have been so generous, not only with your time this morning and your preparation for this hearing but with your expertise and your clear engagement with this issue and desire to help the Federal Government do its work much better in modernizing the IT sector at a time when we so desperately need to do that, for all the reasons, among others, that the pandemic has really laid clear. Thank you for your service, for your expertise, and for your testimony today.

As we wrap up, I will ask each of you this, and I will start with Ms. Wynn. Could each of you describe what, in your opinion, is the greatest challenge presented by the sustained use of legacy IT systems? If you already feel like you have talked about it, just go ahead and say that. But I really do not want to let this opportunity go without giving you all a chance to focus on that.

Ms. Wynn, we will start with you.

Ms. WYNN. Great. Thank you, and thank you again for the honor to testify today. It is a great pleasure of mine to continue to give to the United States Federal Government after 30 years of service.

I would say the greatest challenge presented to us today are agency and department cultures. They must recognize that IT modernization is part of the path forward for the United States government to quickly and securely deliver new or better quality services to the American public. This needs to be done with a positive customer experience, and finally, it must be delivered in a way that improves national security and not poke a hole through it.

Again, it was an honor to be here and to be with my former colleagues as well. Thank you.

Senator HASSAN. Thank you, Ms. Wynn. Mr. Everett.

Mr. EVERETT. I would say I hope that we have covered it well for you. I would summarize by simply saying missed opportunities. To me, this challenge is we are missing opportunities across the board, opportunities to secure our systems, opportunities to entice people with new and innovative skills into government, and opportunities to serve the citizens of the country. All of those, they are these missed opportunities, over and over again, that we were stuck in these systems.

Again, that word I used, technical debt, but that is what it means. It is not the money. As Renee said, it is the culture. It is so many of these things that we are missing out on, these missed opportunities, that we could get simply by doing some basic modernization of systems. The flow-down effect would be really, I think, dramatic in so many different areas.

That is the part that disappoints me, but right now it also excites me, because we have gotten new resources, we have the attention of Congress and other folks. We have some really good, new opportunities right now, and everyone has seen the value that IT can bring to life and to meeting challenges. Just after this last year of dealing with COVID, there are so many things we are able to do because of technology. I think there is a unique time of recognition of that. I would love to see that progress, not pause but accelerate in 2021.

Senator HASSAN. Thank you. Ms. Coleman.

Ms. COLEMAN. Chair Hassan, I think it is a mark of how aligned we all are that when you asked this question I wrote down "culture change" and "missed opportunities," just like Renee and Max. I think that, just to double down on that statement, modern technology allows us to do things not just better but things we could not do before, and I think that is the missed opportunity if we do not modernize.

I will give you one very quick example. The pandemic has illustrated so many areas where government is so critical to the wellbeing of the public. In New Mexico, unemployment claims spiked by 600 percent when people were thrust out of work, and call center workers were sent home, and they were not able to process claims in a timely way.

We had the opportunity to help them with a virtual contact center, which allowed their workers to work from home, but also with chatbots. It let them answer questions in an automated fashion, and take some of that burden off of the call center agents to focus on the higher-value need, and get economic relief into the community quickly.

There are things that can be done that we are not taking advantage of, at every level of government, and I think that the time is now to rethink that. Thank you.

Senator HASSAN. Thank you. Mr. Walsh.

Mr. WALSH. It is hard to imagine a government function that is not somehow tied to IT. As we go along, IT has become more and more complex. If you look back, again to the Voyager probes, those were written with 3,000 lines of COBOL code. We have come a long way since then. Modern technology requires millions, if not billions, of lines of code.

The problem is the longer we wait to modernize, the longer we procrastinate, the more it is going to cost, both in terms of money, in terms of breaches, in terms of security, in terms of lost—to quote my peers—lost opportunities, ways that we could have better served our citizens.

It is an issue of procrastination. We need to act. We need to act now.

Senator HASSAN. Thank you. Thank you to all four of you, for your time and your testimony this morning. To Kevin Walsh, Casey Coleman, Renee Wynn, and Max Everett, your testimony provided really valuable insights on this topic, and your contributions to improving Federal IT systems in a fiscally responsible way are really appreciated.

As I mentioned in my opening statement, this hearing is the first on the costs and challenges presented by reliance on legacy IT systems, and I look forward to continuing this important oversight work, to save taxpayer dollars, to deliver government services more efficiently, and to keep government IT systems secure.

The hearing record will remain open for 15 days, until 5 p.m. on May 12th, for submissions of statements and questions for the record.

This hearing is now adjourned.

[Whereupon, at 11:27 a.m., the Subcommittee was adjourned.]

APPENDIX

Opening Statement as Prepared for Delivery by Chair Maggie Hassan
Emerging Threats and Spending Oversight Subcommittee Hearing:
Controlling Federal Legacy IT Costs and Crafting 21st Century IT Management Solutions
April 27, 2021

Good morning, and thank you to our panel of witnesses for appearing today to discuss controlling federal legacy IT costs and crafting 21st century IT management solutions.

I also want to thank Ranking Member Paul and his staff for working with us on this hearing, and for our continued partnership to address wasteful spending and government inefficiencies. Even though Ranking Member Paul is unable to join us this morning, I look forward to working with him and other members of the Subcommittee to address the threats posed by the federal government's failure to maintain a modern and agile information technology infrastructure.

Today is the first of multiple hearings on federal legacy IT systems. By shining a light on this important issue, I hope that agencies will work to reduce their reliance on costly legacy IT systems in partnership with Congress, the Biden Administration, and industry stakeholders. Today's hearing will focus on identifying the costs and consequences of legacy IT, as well as the institutional barriers to modernization.

According to the Office of Management and Budget and Government Accountability Office, in fiscal year 2020, the federal government spent roughly $90 billion on IT investments and operations. Based on analysis of agency expenditures, legacy IT maintenance costs accounted for one-third – about $29 billion – of total spending. However, the actual cost is estimated to be much greater when we consider legacy IT's negative effects on security, delivery of services, and customer experience.

To frame our discussion, we should have a common definition of legacy IT. Legacy IT describes the federal government's use of old technology or custom systems designed to support insular agency operations. That is, legacy IT includes technology and systems that are no longer supported by industry vendors, as well as those that require additional maintenance or specialized knowledge to operate.

We have seen the consequences of relying on legacy IT systems. For example, in 2014, hackers stole the personal information of more than 20 million people from the Office of Personnel Management, because they were able to breach OPM's vulnerable legacy IT systems that lacked encryption. Despite this breach that was clearly linked to a failure to modernize, OPM still relies on a 34-year old legacy IT system that costs $45 million annually - roughly one-third of OPM's annual IT budget - even though a modern system would only cost $10 million and produce $16 million in cost savings.

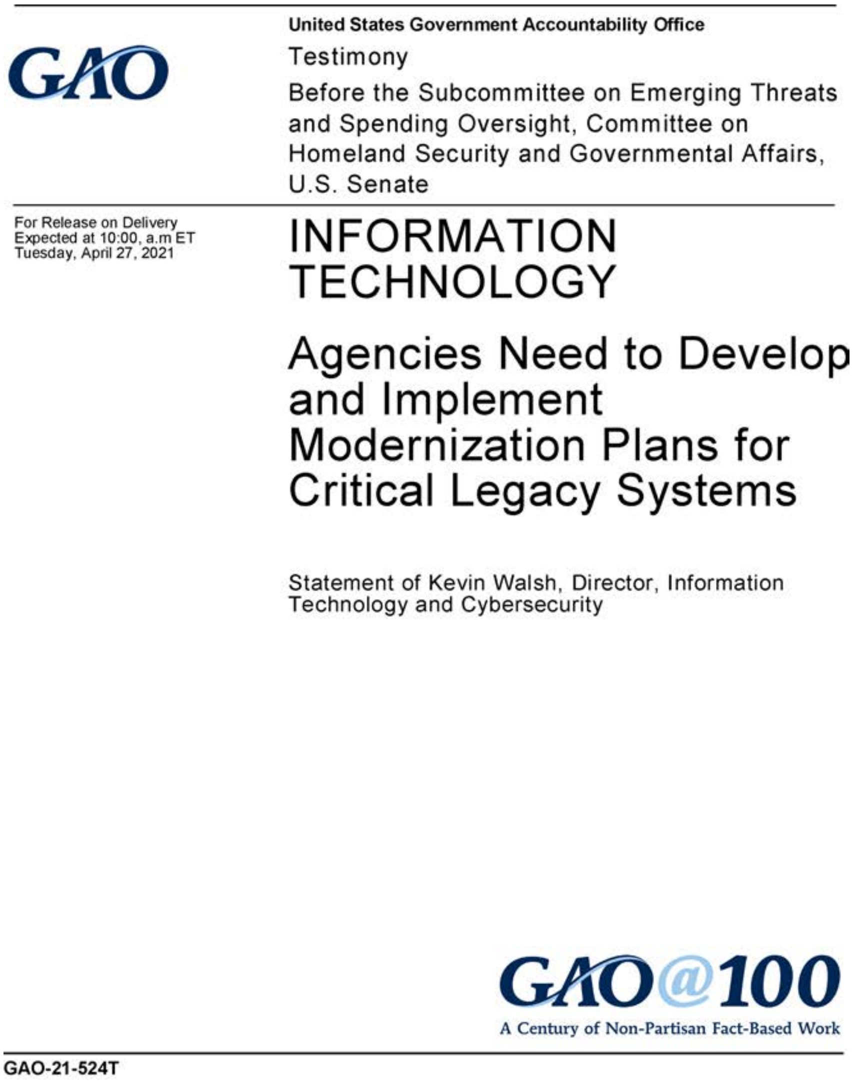
At the Internal Revenue Service, the system used to annually process millions of tax documents is more than 50 years old and relies on a programming language called the "common business-oriented language," or COBOL, which was invented in 1959. In 2018, implementation of the 2017 tax law hit a major roadblock due to a shortage of staff with the specialized knowledge needed to update COBOL-based tax-processing systems. IRS estimates that it costs $15.9 million annually to operate this system and 60 percent of those costs are for labor alone. During the COVID-19 pandemic, IRS faced additional challenges, because many of its aging systems rely on paper rather than digital records, which were inaccessible to IRS employees working remotely. And as a result, the American people felt the burden of delayed tax-returns and economic stimulus payments.

Similarly, in 2016, the Social Security Administration was forced to rehire retirees to maintain the COBOL system used for making payments to beneficiaries and their dependents. These systems cost the Social Security Administration almost $146 million annually to operate. However, the Social Security Administration estimates that it would only cost $25 million over five years to modernize the system, and would significantly improve functionality and security, as well as eliminate the need for specialized programmers.

This begs the question: what are agencies waiting for? What is holding them back from realizing significant cost savings, increasing security, and providing greater customer service delivery through reducing their reliance on legacy IT?

In addition to the costs and consequences of relying on legacy IT systems, today's hearing will also discuss the institutional barriers that prevent agencies from moving forward with their modernization efforts.

Our distinguished panel includes the director of the Government Accountability Office's information technology and cybersecurity team, as well as three former federal agency chief information officers who navigated the challenging IT modernization landscape and successfully moved their agencies away from legacy IT systems. I look forward to hearing from all of our witnesses about how they achieved success by leveraging available resources and being innovative.



United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 10:00, a.m ET
Tuesday, April 27, 2021

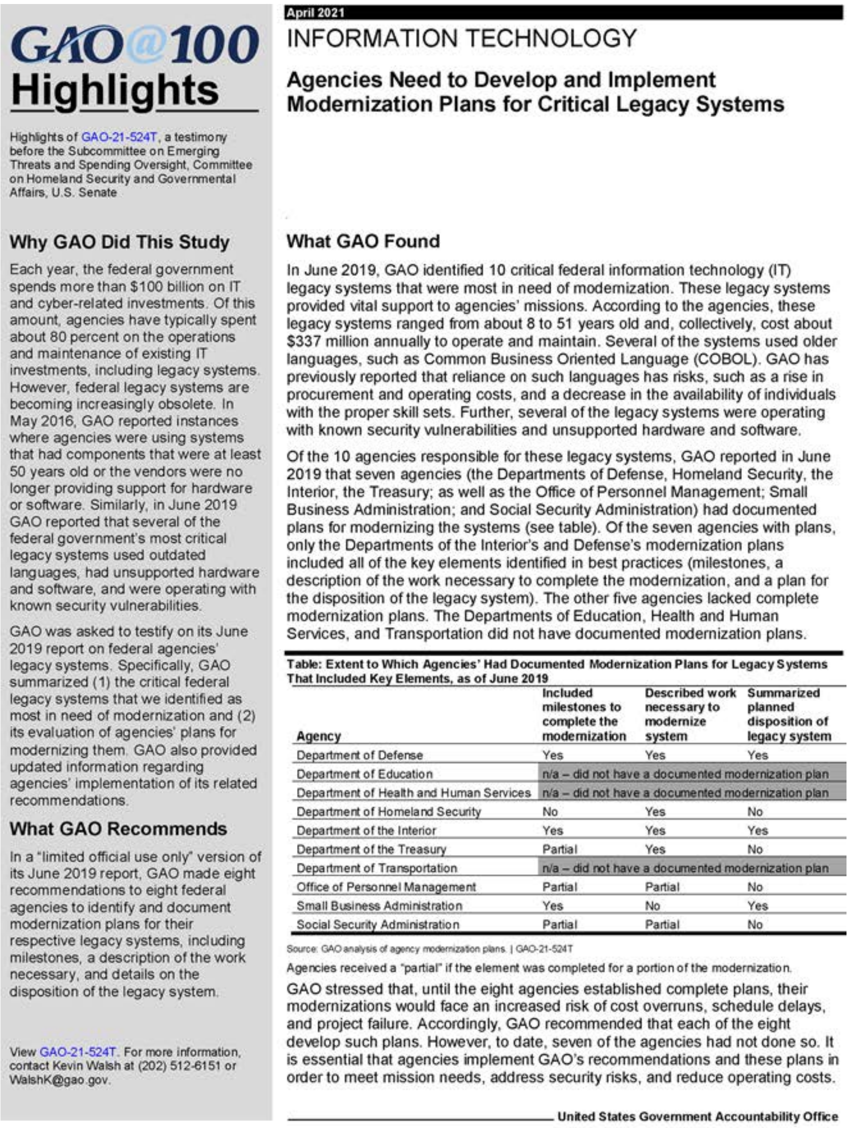
INFORMATION TECHNOLOGY

Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems

Statement of Kevin Walsh, Director, Information Technology and Cybersecurity

A Century of Non-Partisan Fact-Based Work

GAO-21-524T



GAO@100

Highlights

Highlights of GAO-21-524T, a testimony before the Subcommittee on Emerging Threats and Spending Oversight, Committee on Homeland Security and Governmental Affairs, U.S. Senate

April 2021

INFORMATION TECHNOLOGY

Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems

Why GAO Did This Study

Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically spent about 80 percent on the operations and maintenance of existing IT investments, including legacy systems. However, federal legacy systems are becoming increasingly obsolete. In May 2016, GAO reported instances where agencies were using systems that had components that were at least 50 years old or the vendors were no longer providing support for hardware or software. Similarly, in June 2019 GAO reported that several of the federal government's most critical legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.

GAO was asked to testify on its June 2019 report on federal agencies' legacy systems. Specifically, GAO summarized (1) the critical federal legacy systems that we identified as most in need of modernization and (2) its evaluation of agencies' plans for modernizing them. GAO also provided updated information regarding agencies' implementation of its related recommendations.

What GAO Recommends

In a "limited official use only" version of its June 2019 report, GAO made eight recommendations to eight federal agencies to identify and document modernization plans for their respective legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system.

View GAO-21-524T. For more information, contact Kevin Walsh at (202) 512-6151 or WalshK@gao.gov.

What GAO Found

In June 2019, GAO identified 10 critical federal information technology (IT) legacy systems that were most in need of modernization. These legacy systems provided vital support to agencies' missions. According to the agencies, these legacy systems ranged from about 8 to 51 years old and, collectively, cost about $337 million annually to operate and maintain. Several of the systems used older languages, such as Common Business Oriented Language (COBOL). GAO has previously reported that reliance on such languages has risks, such as a rise in procurement and operating costs, and a decrease in the availability of individuals with the proper skill sets. Further, several of the legacy systems were operating with known security vulnerabilities and unsupported hardware and software.

Of the 10 agencies responsible for these legacy systems, GAO reported in June 2019 that seven agencies (the Departments of Defense, Homeland Security, the Interior, the Treasury; as well as the Office of Personnel Management; Small Business Administration; and Social Security Administration) had documented plans for modernizing the systems (see table). Of the seven agencies with plans, only the Departments of the Interior's and Defense's modernization plans included all of the key elements identified in best practices (milestones, a description of the work necessary to complete the modernization, and a plan for the disposition of the legacy system). The other five agencies lacked complete modernization plans. The Departments of Education, Health and Human Services, and Transportation did not have documented modernization plans.

Table: Extent to Which Agencies' Had Documented Modernization Plans for Legacy Systems That Included Key Elements, as of June 2019

Agency	Included milestones to complete the modernization	Described work necessary to modernize system	Summarized planned disposition of legacy system
Department of Defense	Yes	Yes	Yes
Department of Education	n/a – did not have a documented modernization plan		
Department of Health and Human Services	n/a – did not have a documented modernization plan		
Department of Homeland Security	No	Yes	No
Department of the Interior	Yes	Yes	Yes
Department of the Treasury	Partial	Yes	No
Department of Transportation	n/a – did not have a documented modernization plan		
Office of Personnel Management	Partial	Partial	No
Small Business Administration	Yes	No	Yes
Social Security Administration	Partial	Partial	No

Source: GAO analysis of agency modernization plans. | GAO-21-524T

Agencies received a "partial" if the element was completed for a portion of the modernization.

GAO stressed that, until the eight agencies established complete plans, their modernizations would face an increased risk of cost overruns, schedule delays, and project failure. Accordingly, GAO recommended that each of the eight develop such plans. However, to date, seven of the agencies had not done so. It is essential that agencies implement GAO's recommendations and these plans in order to meet mission needs, address security risks, and reduce operating costs.

United States Government Accountability Office

Chair Hassan, Ranking Member Paul, and Members of the Subcommittee:

I am pleased to participate in today's hearing on the federal government's legacy information technology (IT) systems. Each year, the federal government spends more than $100 billion on IT and cyber-related investments. Of this amount, agencies have typically reported spending about 80 percent on the operations and maintenance of existing IT investments, including legacy systems.[1]

However, federal legacy systems are becoming increasingly obsolete. In May 2016, we reported instances where agencies were using systems that had components that were at least 50 years old or the vendors were no longer providing support for hardware or software.[2] Likewise, in June 2019, we reported that several of the federal government's most critical legacy systems used outdated languages, had unsupported hardware and software, and were operating with known security vulnerabilities.[3]

As you requested, my testimony today discusses the results from our June 2019 report on federal agencies' legacy systems. Specifically, it summarizes (1) the critical federal legacy systems that we identified as most in need of modernization and (2) our evaluation of agencies' plans for modernizing them. Detailed information on the objectives, scope, and methodology for that work can be found in the issued report. In addition, this statement includes updated information regarding agencies' implementation of related recommendations that we made in a "limited official use only" version of the June 2019 report.

We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained

[1] The provisions commonly referred to as the Modernizing Government Technology (MGT) Act define a legacy IT system as a system that is outdated or obsolete. *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1586-94 (2017).

[2] GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

[3] GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: June 11, 2019).

provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Historically, the federal government has had difficulties acquiring, developing, and managing IT investments.[4] Further, federal agencies have struggled with appropriately planning and budgeting for modernizing legacy systems; upgrading underlying infrastructure; and investing in high quality, lower cost service delivery technology. The consequences of not updating legacy systems has contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs.

- **Security risks**. Legacy systems may operate with known security vulnerabilities that are either technically difficult or prohibitively expensive to address. In some cases, vendors no longer provide support for hardware or software, creating security vulnerabilities and additional costs. For example, in November 2017, the Department of Education's (Education) Inspector General identified security weaknesses that included the department's use of unsupported operating systems, databases, and applications.[5] By using unsupported software, the department put its sensitive information at risk, including the personal records and financial information of millions of federal student aid applicants.[6]
- **Unmet mission needs**. Legacy systems may not be able to reliably meet mission needs because they are outdated or obsolete. For

[4] As a result of the difficulties in acquiring, developing, and managing IT investments the federal government has experienced, we identified "Improving the Management of IT Acquisitions and Operations" as a high-risk area in February 2015. GAO's high-risk program identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement, or in need of transformation to address economy, efficiency, or effectiveness challenges. Every 2 years, we issue an update that describes the status of these high-risk areas and actions that are still needed to assure further progress, and identifies new high-risk areas needing attention by Congress and the executive branch. We continue to identify this area as high risk. GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[5] Department of Education, Office of Inspector General, *FY 2018 Management Challenges*, (Washington, D.C.: November 2017).

[6] According to Education's Office of General Counsel, Education has developed corrective action plans to address the Inspector General's recommendation.

instance, in 2016, the Department of State's (State) Inspector General reported on the unreliability of the Bureau of Consular Affairs' legacy systems.[7] Specifically, during the summers of 2014 and 2015, outages in the legacy systems slowed and, at times, stopped the processing of routine consular services such as visa processing. For example, in June 2015, system outages caused by a hardware failure halted visa processing for 13 days, creating a backlog of 650,000 visas.

- **Staffing issues.** In order to operate and maintain legacy systems, staff may need experience with older technology and programming languages, such as the Common Business Oriented Language (COBOL).[8] Agencies have had difficulty finding employees with such knowledge and may have to pay a premium for specialized staff or contractors. For example, we reported in May 2016 that the Social Security Administration (SSA) had to rehire retired employees to maintain its COBOL systems.[9]

  Further, having a shortage of expert personnel available to maintain a critical system creates significant risk to an agency's mission. For instance, we reported in June 2018 that the Internal Revenue Service (IRS) was experiencing shortages of staff with the skills to support key tax processing systems that used legacy programming languages.[10] These staff shortages not only posed risks to the operation of the key tax processing systems, but they also hindered the agency's efforts to modernize its core tax processing system.

[7] U.S. Department of State, Office of Inspector General, *Inspection of the Bureau of Consular Affairs, Office of Consular Systems and Technology*, ISP-I-17-04, (Arlington, VA: December 2016).

[8] COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language. See Gartner, *IT Market Clock for Application Development,* August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

[9] GAO-16-468.

[10] GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing*, GAO-18-298 (Washington, D.C.: June 28, 2018).

- **Increased costs.** The cost of operating and maintaining legacy systems increases over time. The issue of cost is linked to security risks, unmet mission needs, and staffing issues, as described above, either because the other issues directly raise costs or, as in the case of not meeting mission needs, the agency is not receiving a favorable return on investment. Further, in an era of constrained budgets, the high costs of maintaining legacy systems could limit agencies' ability to modernize and develop new or replacement systems.

Agencies reported that they consider several factors prior to deciding whether to modernize a legacy system. In particular, they reported evaluating factors such as the inherent risks, the criticality of the system, the associated costs, and the system's operational performance.

- **Risks**. Agencies consider the risks associated with maintaining the legacy system as well as modernizing the legacy system. For instance, agencies may prioritize the modernization of legacy systems that have security vulnerabilities or software that is unsupported by the vendor.[11] However, limited system accessibility may also reduce the need to modernize a legacy system. For example, air-gapped systems, which are systems that are isolated from the internet, may mitigate a legacy system's cybersecurity risk by preventing remote hackers from having system access.[12]

  Conversely, we have also reported that air-gapped systems are not necessarily secure: they could potentially be accessed by other means than the internet, such as through Universal Serial Bus devices.[13] Even so, removing the threat of remote access is a mitigation technique used by agencies such as the Nuclear Regulatory Commission (NRC). According to NRC, the agency reduced the riskiness of using computers with unsupported operating systems by putting these computers on isolated networks or by disconnecting them from networks entirely.

[11] When computer systems or software are no longer supported, the vendor of the product ceases to provide patches, security fixes, or updates, leaving system vulnerabilities open to exploitation.

[12] Michael DePhillips and Susan Pepper, "Computer Security – Indirect Vulnerabilities and Threat Vectors (Air-Gap In-depth)" (paper presented at the International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, Vienna, Austria: November 2017).

[13] GAO, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

- **Criticality**. Agencies consider how critical the system is to the agency's mission. Several agencies stated that they would consider how essential a legacy system is to their agencies' missions before deciding to modernize it. For example, the Department of Health and Human Services (HHS) stated that, when deciding to modernize a legacy system, it considers the degree to which core mission functions of the agency or other agencies are dependent on the system. Similarly, Department of Energy officials noted that the department is required to maintain several legacy systems associated with the storage of its nuclear waste.
- **Costs**. Agencies consider the costs of maintaining a legacy system and modernizing the system. For example, according to the Department of Veterans Affairs (VA), there are systems for which a life-cycle cost analysis of the legacy system may show that the cost to modernize exceeds the projected costs to maintain the system. Similarly, the Department of Defense (DOD) noted that, before deciding on a modernization solution, it is important to assess the costs of the transition to a new or replacement solution.

  An agency also may decide to modernize a system when there is the potential for cost savings to be realized with a modernization effort. For example, HHS stated that it may pursue the modernization of a legacy system if the department anticipates reductions in operations and maintenance costs due to efficiencies gained through the modernization.
- **Performance**. Before making the decision to modernize, agencies consider the legacy system's operational performance. Specifically, if the legacy system is performing poorly, the agency may decide to modernize it. For example, the Department of Transportation (Transportation) stated that, if a legacy system is no longer functioning properly, it should be modernized. In addition, HHS noted that the ability to improve the functionality of the legacy system could be a reason to modernize it.

Congress and the Executive Branch Have Made Efforts to Modernize Federal IT

Congress and the executive branch have initiated several efforts to modernize federal IT, including:

- **Identification of High Value Assets**. In December 2018, OMB issued a memorandum that provided guidance regarding the establishment and enhancement of the High Value Asset program.[14] It stated that the program is to be operated by the Department of Homeland Security (DHS) in coordination with OMB. The guidance required agencies to identify and report these assets (which may include legacy systems), assess them for security risks, and remediate any weaknesses identified, including those associated with obsolete or unsupported technology.[15]

- **Enactment of provisions commonly referred to as the Modernizing Government Technology (MGT) Act**. To help further agencies' efforts to modernize IT, in December 2017, Congress and the President enacted a law to authorize the availability of funding mechanisms to improve, retire, or replace existing IT systems to enhance cybersecurity and to improve efficiency and effectiveness. The law, known as the MGT Act, authorizes agencies to establish working capital funds for use in transitioning from legacy systems, as well as for addressing evolving threats to information security.[16] The law also created the Technology Modernization Fund, within the Department of the Treasury (Treasury), from which agencies can "borrow" money to retire and replace legacy systems, as well as acquire or develop systems.

  Subsequently, in February 2018, OMB issued guidance for agencies to implement the MGT Act.[17] The guidance was intended to provide agencies additional information regarding the Technology Modernization Fund, and the administration and funding of the related IT working capital funds. Specifically, the guidance allowed agencies

[14] OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018). This memorandum rescinded the previous guidance on High Value Assets, M-16-04 and M-17-09.

[15] According to OMB's December 2018 guidance, an agency may designate federal information or an information system as a High Value Asset when one or more of these categories apply to it: (1) the information or information system that processes, stores, or transmits the information is of high value to the federal government or its adversaries; (2) the agency that owns the information or information system cannot accomplish its primary mission essential functions within expected timelines without the information or information system; and (3) the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

[16] *National Defense Authorization Act for Fiscal Year 2018*, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1586-94 (2017).

[17] OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

to begin submitting initial project proposals for modernization on February 27, 2018.

In addition, in accordance with the MGT Act, the guidance provides details regarding a Technology Modernization Board, which is to consist of (1) the Federal Chief Information Officer (CIO) (Chair); (2) a senior official with IT development technical expertise from GSA; (3) a member of DHS's National Protection and Program Directorate;[18] and (4) four federal employees with technical expertise in IT development, financial management, cybersecurity and privacy, and acquisition, appointed by the Director of OMB.[19]

In December 2019, we reported that Congress had appropriated $125 million to the fund, but that challenges with covering the cost of operating the fund had resulted in fewer funds being available than anticipated for the new projects.[20] On March 11, 2021, Congress and the President enacted legislation that appropriated an additional $1 billion to be available until September 30, 2025, to carry out the purposes of the fund.[21]

As of April 2021, the Technology Management Fund Board had approved approximately $89 million for 11 IT modernization projects across seven agencies: the Department of Agriculture, the Department of Energy, DHS, the Department of Housing and Urban Development (HUD), the Department of Justice, the Department of Labor, and GSA. For example, the board approved $13.9 million for HUD to modernize a mainframe and five COBOL-based applications that are expensive to maintain. According to the board's website,

[18] The National Protection and Program Directorate was the DHS component responsible for addressing physical and cyber infrastructure protection. The Cybersecurity and Infrastructure Security Agency Act of 2018 renamed the National Protection and Program Directorate as the Cybersecurity and Infrastructure Security Agency and established a director and responsibilities for the agency.

[19] As of April 2021, these four employees were the Department of Agriculture's Farm Production and Conservation Mission Area Assistant CIO, National Science Foundation's Deputy Assistant Director for Computer and Information Science and Engineering, National-Geospatial Intelligence Agency's Deputy Chief Technology Officer, and VA's Chief Technology Officer.

[20] GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects*, GAO-20-3 (Washington, D.C.: Dec. 12, 2019).

[21] American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021).

without these funds, HUD would not have been able to pursue this project for several years.

GAO Identified the 10 Most Critical Federal Legacy Systems; Agencies Often Lacked Complete Plans for Their Modernization

Of 65 critical federal legacy systems that agencies identified for our June 2019 report (further discussed in appendix I), we determined the 10 that were most in need of modernization.[22] These legacy systems provided vital support to their agencies' missions.

According to the agencies, at the time, these 10 legacy systems ranged from about 8 to 51 years old and, collectively, cost approximately $337 million annually to operate and maintain.[23] Several of the systems used older languages, such as COBOL and assembly language code.[24] However, as we reported in June 2018, reliance on assembly language code and COBOL has risks, such as a rise in procurement and operating costs, and a decrease in the availability of individuals with the proper skill sets.[25]

Further, several of these legacy systems were operating with known security vulnerabilities and unsupported hardware and software. For example, DHS's Federal Emergency Management Agency performed a security assessment on its selected legacy system in September 2018.

[22] To identify the 10 most critical legacy systems in need of modernization, we collected information on 65 of the most critical federal legacy systems and assigned point values based on system attributes, including a system's age, hardware's age, system criticality, and security risk (see appendix I for the full list of 65 systems). We then selected the 10 systems with the highest scores as the most critical legacy systems in need of modernization.

[23] SSA was unable to isolate the costs for just System 10 and, as a result, this number includes the cost of operating some of SSA's other mainframe systems.

[24] As we reported in May 2016, assembly language code is a low-level computer language initially used in the 1950s. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language may only run on the type of computer for which they were originally developed.

[25] GAO, *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks to Tax Processing,* GAO-18-298 (Washington, D.C.: June 28, 2018).

This review found 249 reported vulnerabilities, of which 168 were considered high or critical risk to the network.

With regard to unsupported hardware and software, the Department of the Interior's (Interior) system contained obsolete hardware that was not supported by the manufacturers. Moreover, the system's original hardware and software installation did not include any long-term vendor support. Thus, any original components that remained operational may have had long-term exposure to security and performance weaknesses.

Table 1 provides a generalized list of each of the 10 critical legacy systems that we identified, as of June 2019, as well as agency-reported system attributes, including the system's age, hardware's age, system criticality, and security risk. (Due to sensitivity concerns, we substituted a numeric identifier for the system names and are not providing detailed descriptions). Appendix II provides additional generalized agency-reported details on each of these 10 legacy systems, as of June 2019.

Table 1: The 10 Critical Federal Legacy Systems Most in Need of Modernization, as of June 2019

Agency	System name[a]	System description[a]	Age of system, in years	Age of oldest hardware, in years	System criticality (according to agency)	Security risk (according to agency)
Department of Defense	System 1	A maintenance system that supports wartime readiness, among other things	14	3	Moderately high	Moderate
Department of Education	System 2	A system that contains student information	46	3	High	High
Department of Health and Human Services	System 3	An information system that supports clinical and patient administrative activities	50	Unknown[b]	High	High
Department of Homeland Security	System 4	A network that consists of routers, switches, and other network appliances	Between 8 and 11[c]	11	High	High
Department of the Interior	System 5	A system that supports the operation of certain dams and power plants	18	18	High	Moderately high
Department of the Treasury	System 6	A system that contains taxpayer information	51	4	High	Moderately low
Department of Transportation	System 7	A system that contains information on aircraft	35	7	High	Moderately high
Office of Personnel Management	System 8	Hardware, software, and service components that support information technology applications and services	34	14	High	Moderately low
Small Business Administration	System 9	A system that controls access to applications	17	10	High	Moderately high
Social Security Administration	System 10	A group of systems that contain information on Social Security beneficiaries	45	5	High	Moderate

Source: GAO analysis of agency data. | GAO-21-524T

Key:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical and the highest risk).

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

[a]Due to sensitivity concerns, we substituted a numeric identifier for the system names and only provided general details.

[b]The agency stated that the system's hardware had various refresh dates and that it was not able to identify the oldest hardware.

[c]The agency stated that the majority of the network's hardware was purchased between 2008 and 2011.

The Majority of Agencies Lacked Complete Plans for Modernizing the Most Critical Legacy Systems

Given the age of the hardware and software in legacy systems, the systems' criticality to agency missions, and the security risks posed by operating aging systems, it is imperative that agencies carefully plan for their successful modernization. Documenting modernization plans in sufficient detail increases the likelihood that modernization initiatives will succeed. Our review of government and industry best practices for the modernization of federal IT[26] stressed that agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.

Of the 10 identified agencies with critical systems most in need of modernization, as of June 2019, the majority lacked complete plans for modernizing the systems. Specifically, seven agencies (DOD, DHS, Interior, Treasury, the Office of Personnel Management (OPM), the Small Business Administration (SBA), and SSA) had documented

[26] GSA, Unified Shared Services Management, *Modernization and Migration Management (M3) Playbook* (Aug. 3, 2016); and *M3 Playbook Guidance* (Aug. 3, 2016); American Technology Council, *Report to the President on Federal IT Modernization* (Dec. 13, 2017); OMB, *Management of Federal High Value Assets*, M-17-09 (Washington, D.C.: Dec. 9, 2016); American Council for Technology-Industry Advisory Council, *Legacy System Modernization: Addressing Challenges on the Path to Success* (Fairfax, VA: Oct. 7, 2016); and Dr. Gregory S. Dawson, Arizona State University, IBM Center for The Business of Government, *A Roadmap for IT Modernization in Government* (Washington, D.C.: 2018).

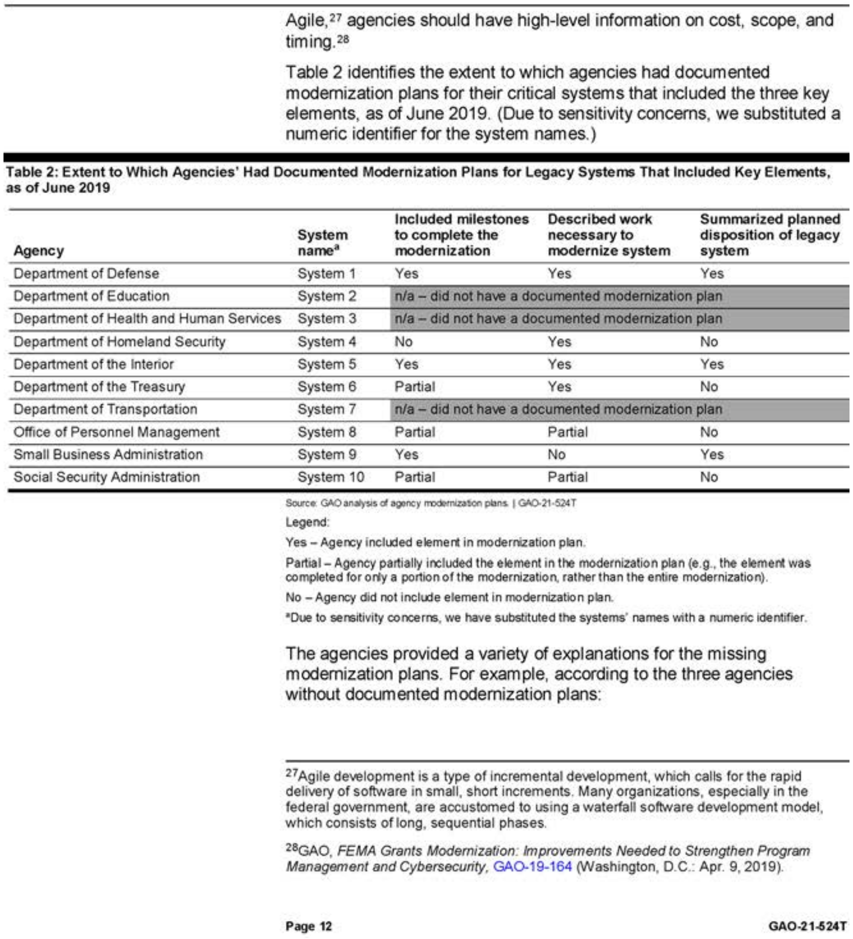
modernization plans for their respective critical legacy systems and three did not have documented plans. The three agencies that did not have documented modernization plans for their critical legacy systems were: (1) Education, (2) HHS, and (3) Transportation.

Of the seven agencies with documented plans, DOD and Interior had modernization plans that addressed each of the three key elements. For example, Interior submitted documentation of both completed and forthcoming milestones leading to the deployment of the modernized system. The department also provided a list of the mandatory requirements for the updated system, as well as the work that needed to be performed at each stage of the project, including the disposition of the legacy system.

Likewise, DOD provided documentation of the milestones and the work needed to complete the modernization of its legacy system. In addition, the documentation discussed the department's plans for the disposition of the legacy system.

While the other five agencies—Treasury, DHS, OPM, SBA, and SSA—had developed modernization plans for their respective legacy systems, their plans did not fully address one or more of the three key elements. For instance, the modernization plan that DHS's Federal Emergency Management Agency developed for its selected legacy system described the work that the department needed to accomplish; however, the plan did not include the associated milestones or the disposition of the legacy system. Similarly, SBA included milestones and a plan for the disposition of the legacy system, but did not include a description of the work necessary to accomplish the modernization.

Treasury, OPM, and SSA partially included one or more of the key elements in their modernization plans. For instance, OPM's and SSA's plans included upcoming milestones for one part of the initiative, but not for the entire effort. Similarly, OPM's modernization plans only described a portion of the work necessary to complete each modernization initiative. Further, none of these four agencies' modernization plans included considerations for the disposition of legacy system components following the completion of the modernization initiatives. While agencies may be using development practices that minimize initial planning, such as



Agile,[27] agencies should have high-level information on cost, scope, and timing.[28]

Table 2 identifies the extent to which agencies had documented modernization plans for their critical systems that included the three key elements, as of June 2019. (Due to sensitivity concerns, we substituted a numeric identifier for the system names.)

Table 2: Extent to Which Agencies' Had Documented Modernization Plans for Legacy Systems That Included Key Elements, as of June 2019

Agency	System name[a]	Included milestones to complete the modernization	Described work necessary to modernize system	Summarized planned disposition of legacy system
Department of Defense	System 1	Yes	Yes	Yes
Department of Education	System 2	n/a – did not have a documented modernization plan		
Department of Health and Human Services	System 3	n/a – did not have a documented modernization plan		
Department of Homeland Security	System 4	No	Yes	No
Department of the Interior	System 5	Yes	Yes	Yes
Department of the Treasury	System 6	Partial	Yes	No
Department of Transportation	System 7	n/a – did not have a documented modernization plan		
Office of Personnel Management	System 8	Partial	Partial	No
Small Business Administration	System 9	Yes	No	Yes
Social Security Administration	System 10	Partial	Partial	No

Source: GAO analysis of agency modernization plans. | GAO-21-524T

Legend:

Yes – Agency included element in modernization plan.

Partial – Agency partially included the element in the modernization plan (e.g., the element was completed for only a portion of the modernization, rather than the entire modernization).

No – Agency did not include element in modernization plan.

[a] Due to sensitivity concerns, we have substituted the systems' names with a numeric identifier.

The agencies provided a variety of explanations for the missing modernization plans. For example, according to the three agencies without documented modernization plans:

[27] Agile development is a type of incremental development, which calls for the rapid delivery of software in small, short increments. Many organizations, especially in the federal government, are accustomed to using a waterfall software development model, which consists of long, sequential phases.

[28] GAO, *FEMA Grants Modernization: Improvements Needed to Strengthen Program Management and Cybersecurity,* GAO-19-164 (Washington, D.C.: Apr. 9, 2019).

- Education's modernization plans were pending the results of a comprehensive IT visualization and engineering project that would determine which IT systems and services could be feasibly modernized, consolidated, or eliminated;
- HHS had entered into a contract to begin a modernization initiative, but had not yet completed its plans; and
- Transportation had solicited information from industry to determine whether the agency's ideas for modernization were feasible.

Of the five agencies which had plans that lacked key elements, officials within SSA's Office of the CIO stated that the agency had yet to complete its modernization planning, even though modernization efforts were currently underway. The officials said that they would update the planning documentation and make further decisions as the modernization effort progresses.

Officials within the DHS Federal Emergency Management Agency's Office of the CIO stated that the office's plans for modernizing the system we reviewed (System 4) were contingent on receiving funding and being able to allocate staffing resources to planning activities. According to the officials, the agency was also integrating its plans for modernizing System 4 with the management of the rest of the agency's systems.

Similarly, Treasury officials stated that IRS's efforts to complete planning for the remaining modernization activities had been delayed due to budget constraints. In addition, officials within OPM's Office of the CIO stated that its modernization plan did not extend to fiscal year 2019 because there were changes in leadership during the creation of the plan, and because of uncertainty in funding amounts.

As we noted in our report, we recognize that system modernizations are dependent on funding; however, it is important for agencies to prioritize funding for the modernization of these critical legacy systems. In addition, Congress provided increased authority for agencies to fund such modernization efforts through the MGT Act's Technology Modernization Fund and the related IT working capital funds.

Until the agencies establish complete legacy system modernization plans that include milestones, describe the work necessary to modernize the system, and detail the disposition of the legacy system, the agencies' modernization initiatives will have an increased likelihood of cost overruns, schedule delays, and overall project failure. Project failure would be particularly detrimental in these 10 cases, not only because of wasted resources, but also because it would prolong the lifespan of increasingly vulnerable and obsolete systems, exposing the agency and system clients to security threats and potentially significant performance issues.

Given these risks, in June 2019, we issued a "limited official use only" report that we issued concurrently with the June 2019 report that contained eight recommendations to eight federal agencies to identify and document modernization plans for their respective legacy systems. These plans were to include milestones, a description of the work necessary, and details on the disposition of the legacy system. However, as of April 2021, seven of the eight agencies had not implemented the recommendations.

Further, agencies may not have effectively planned for the modernization of legacy systems, in part, because they were not required to. As we reported in May 2016, agencies were not required to identify, evaluate, and prioritize existing IT investments to determine whether they should be kept as-is, modernized, replaced, or retired.[29] Accordingly, we recommended that OMB direct agencies to identify legacy systems needing to be replaced or modernized.

As of April 2021, OMB had not implemented this recommendation. OMB staff stated that agencies were directed to manage the risk to High Value Assets associated with legacy systems in OMB's December 2018 guidance.[30] However, while OMB's guidance does direct agencies to identify, report, assess, and remediate issues associated with High Value Assets, it does not require agencies to do so for all legacy systems. Until OMB requires agencies to do so, the federal government will continue to run the risk of continuing to maintain investments that have outlived their effectiveness.

In summary, our June 2019 report emphasized the need and importance for agencies to develop a complete plan to modernize their federal legacy systems. Due to the criticality and possible cybersecurity risks posed by operating aging systems, having a plan that includes how and when the agency plans to modernize is vital. In the absence of such plans, the agencies increased the likelihood of cost overruns, schedule delays, and

[29] GAO-16-468.

[30] OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

overall project failure. Such outcomes would be particularly detrimental because of the importance of these systems to agency missions.

In this regard, in June 2019, we recommended that the eight federal agencies identify and document modernization plans for their respective legacy systems, including milestones, a description of the work necessary, and details on the disposition of the legacy system. It is essential that agencies implement our recommendations and these plans in order to meet mission needs, address security risks, and reduce operating costs.

Chair Hassan, Ranking Member Paul, and Members of the Subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have.

GAO Contact and Staff Acknowledgments

If you or your staff have any questions about this testimony, please contact Kevin C. Walsh, Director of Information Technology and Cybersecurity, at (202) 512-6151 or walshk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to this testimony are Jessica Waselkow (Assistant Director), Ashfaq Huda (Analyst-in-Charge), Andrew Avery, Sharhonda Deloach, Rebecca Eyler, and Scott Pettis.

Appendix I: The 24 Chief Financial Officers Act Agencies' Critical Legacy Systems Most in Need of Modernization, as of June 2019

Each of the 24 Chief Financial Officers Act[1] agencies identified their agency's critical legacy systems most in need of modernization. The agencies identified a total of 65 such systems.[2] The agencies also identified various attributes of the legacy systems, including the systems' age, hardware age,[3] system criticality, and security risk. Table 3 provides a generalized list of the critical legacy systems most in need of modernization, as identified by the agencies as of June 2019, as well as selected factors related to each system's age and criticality. (Due to sensitivity concerns, we substituted alphanumeric identifiers for the names of the agencies' systems. Specifically, we assigned a number to identify each of the 10 critical legacy systems most in need of modernization that we discussed in our report and we assigned a letter or letters to identify the remaining 55 systems.)

Table 3: Combined List of Agencies' Critical Legacy Systems Most in Need of Modernization, as of June 2019

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
Department of Agriculture	System A	8	Unknown[b]	High	Moderately low
Department of Commerce	System B	16	5	High	High

[1] The 24 federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. 31 U.S.C. §901(b).

[2] Most agencies provided a list of three legacy systems in need of modernization. However, the Department of Education reported four legacy systems, the Department of Commerce reported two legacy systems, and the Departments of Agriculture and Energy each reported one legacy system. The U.S. Agency for International Development stated that it did not have any legacy systems.

[3] A legacy system may run on updated hardware and, thus, the system's age and hardware age may not be the same.

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
	System C	25	7	High	Low
Department of Defense	System 1	14	3	Moderately high	Moderate
	System D	55	5	High	Low
	System E	33	12	High	Moderately low
Department of Education	System 2	46	3	High	High
	System F	13	12	High	Moderately high
	System G	25	5	High	High
	System H	24	17	Moderate	High
Department of Energy	System I	32	2	High	Low
Department of Health and Human Services	System 3	50	Various[c]	High	High
	System J	21	Unknown[b]	High	Moderate
	System K	7	8	High	Moderate
Department of Homeland Security	System 4	11	11	High	High
	System L	9	2	High	Moderately low
	System M	6	1	High	Low
Department of Housing and Urban Development	System N	42	2	High	Moderate
	System O	44	2	High	Moderate
	System P	44	2	High	Moderate
Department of Justice	System Q	21	10	High	High
	System R	38	7	High	Moderately low
	System S	49	6	Moderately high	Low
Department of Labor	System T	14	9	High	Low
	System U	21	10	High	Low
	System V	15	3	High	Moderate
Department of State	System W	24	5	High	Moderate
	System X	21	5	Moderately high	Moderate
	System Y	20	3	Moderately high	Moderate
Department of the Interior	System 5	18	18	High	Moderately high
	System Z	29	9	High	High
	System AA	23	23	Moderately high	Low
Department of the Treasury	System 6	51	4	High	Moderately low
	System AB	13	10	Moderate	Moderate
	System AC	10	8	High	Moderately low
Department of Transportation	System 7	35	7	High	Moderately high
	System AD	17	4	High	Moderately high

Agency	System name[a]	Age of system, in years	Age of oldest hardware installed, in years	System criticality (as determined by agency)	Security risk (as determined by agency)
	System AE	19	n/a[b]	High	High
Department of Veterans Affairs	System AF	31	3	High	Low
	System AG	49	2	High	Moderately low
	System AH	31	4	High	Moderate
Environmental Protection Agency	System AI	24	1	High	Low
	System AJ	17	1	High	Low
	System AK	14	1	High	Low
General Services Administration	System AL	39	2	High	Low
	System AM	5	10	High	Moderate
	System AN	8	Unknown[b]	High	Moderate
National Aeronautics and Space Administration	System AO	10	13	High	High
	System AP	About 19	31	Moderately high	Moderately low
	System AQ	6	6	High	Low
Nuclear Regulatory Commission	System AR[d]	11	7	Moderately high	Moderate
	System AS[d]	20	2	Moderately high	Moderate
	System AT	15	9	Moderately high	Moderately low
National Science Foundation	System AU	18	2	High	Moderately low
	System AV	18	2	Moderate	Moderately low
	System AW	22	2	Moderate	Moderate
Office of Personnel Management	System 8	34	6	High	Moderately low
	System AX	29	6	High	Moderately high
	System AY	21	6	High	Moderately low
Small Business Administration	System 9	17	10	High	Moderately high
	System AZ	13	10	Moderately high	Moderately high
	System BA	15	3	High	Moderately high
Social Security Administration	System 10	45	5	High	Moderate
	System BB	34	5	High	Moderate
	System BC	38	4	High	Moderate
U.S. Agency for International Development	n/a – Agency stated that it does not have any legacy systems.				

Source: GAO analysis of agency documentation. | GAO-21-524T

Key:

Agencies reported the system criticality and security risk on a scale of 1 to 5 (with 5 being the most critical or the highest risk). We assigned the following based on those numbers.

Low-1: According to the agency, system has low security risk or criticality.

Moderately low-2: According to the agency, system has moderately low security risk or criticality.

Moderate-3: According to the agency, system has moderate security risk or criticality.

Moderately high-4: According to the agency, system has moderately high security risk or criticality.

High-5: According to the agency, system has high security risk or criticality.

[a]Due to sensitivity concerns, we substituted an alphanumeric identifier for the system names.

[b]The agency procures services from a vendor or another agency and was not able to get the information from the vendor.

[c]The agency stated that the system's hardware had various refresh dates and was not able to identify the oldest hardware.

[d]This system has been decommissioned since the agency reported it to us.

Appendix II: Profiles of the 10 Critical Legacy Systems Most in Need of Modernization, as of June 2019

This appendix provides additional details on the 10 critical legacy systems with the greatest need for modernization, as we identified during our June 2019 review. The profiles of each system describe (1) the system's purpose, (2) the reason that the system needs to be modernized, (3) the agency's plans for modernization, and (4) possible benefits to be realized once the system is modernized.

Department of Defense—U.S. Air Force

Reported number of users: Approximately [illegible]

Initial year of implementation: [illegible]

System hardware under warranty? Agency did not know

Software vendor supported? No

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): Moderately high

System security risk (as determined by agency): Moderate

Reported annual operating costs: $21.8 million

Reported annual labor costs: $[illegible] million

Reported cost of modernization: $[illegible] million

Potential cost savings: $34 million annually

Other benefits: Increased functionality, increased aircraft touch time and availability

Status of modernization plans: Agency had documented modernization plans that included milestones to complete the modernization, description of the work necessary to modernize the legacy system, and plans for the disposition of the legacy system.

Source: GAO analysis of agency documentation and interviews as of June 2019. | GAO-21-524T

System 1, as of June 2019

The Department of Defense (DOD)—U.S. Air Force's System 1 provided configuration control and management to support wartime readiness and operational support of aircraft, among other things.

According to Air Force documentation, the cost to maintain and sustain the system had been steadily increasing due to several factors, including (1) costs associated with maintaining and operating the system's infrastructure and the manpower to maintain the legacy code; and (2) the difficulty and cost of experienced Common Business Oriented Language (COBOL)[4] programmers, poor legacy documentation, and an aging infrastructure and code. In addition, the system ran on a mainframe that was hosted by another agency. As a result of these issues, Air Force officials expected annual costs to rise from $21.8 million in 2018 to approximately $35 million beginning in 2020.

In September 2018, the Air Force awarded a contract to modernize and migrate the system to a cloud environment by September 2019. DOD contractors developed a project plan for the modernization that contained goals and outlined how the contractor planned to move through the modernization process, listing out sequential tasks leading to project completion. In addition, it outlined milestones from the starting point through implementation, and provided for the disposition of the legacy system. After the migration, as funding allowed, the Air Force planned to incrementally transform the system's COBOL code to a more modern language.

Air Force program office officials stated that the modernized system would save the agency over $34 million a year, resulting in $356 million saved over a 10-year period. Officials also noted that, given the savings, the modernization would pay for itself in only 5 months. The Air Force also expected increased functionality with this modernization leading to

[4] COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading information technology research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language. See Gartner, *IT Market Clock for Application Development*, August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

increased aircraft touch time[5] and aircraft availability by enabling adoption of new technologies.

[5] Aircraft touch time is the time spent performing aircraft maintenance tasks.

Department of Education—Federal Student Aid

Reported number of users: Over 35 million student applications annually and thousands of other users

Initial year of implementation: 1973

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: $40.8 million

Reported annual labor costs: $2.0 million

Reported cost of modernization: Agency had not determined costs

Potential cost savings: Agency had not calculated

Other benefits: Integration across the enterprise, improved cybersecurity and data protection, reduced system complexity, and increased efficiency

Status of modernization plans: Agency did not have a modernization plan

Source: GAO analysis of agency documentation and interviews with agency officials. | GAO-21-524T

System 2, as of June 2019

The Department of Education's (Education) System 2 processed and stored student information and supported the processing of federal student aid applications.

Education first implemented System 2 in 1973.[6] Agency officials stated that the system ran approximately 1 million lines of Common Business Oriented Language (COBOL)[7] on an IBM mainframe. COBOL is a legacy language that can be costly to maintain. The department noted that 18 contractors were employed to maintain the COBOL programming language for this and another system. At the time, Education officials stated that the agency would like to modernize System 2 to eliminate reliance on COBOL, simplify user interactions, improve integration with other applications, respond to changing business requirements more quickly, and decrease development and operational costs.

Education officials stated that the agency intended to modernize System 2 as part of its Next Generation Financial Services Environment initiative. This initiative was to modernize Federal Student Aid's technical and operational architecture and improve the customer experience. The agency expected to consolidate all customer-facing websites and implement a new loan servicing platform to benefit federal student loans.

As of June 2019, Education had not developed a plan for the modernization of System 2. According to agency officials, at the time, modernization plans were pending the results of a comprehensive information technology (IT) visualization and engineering project that will determine which IT systems and services could be feasibly modernized, consolidated, or eliminated.

While Education had not calculated the specific cost savings associated with modernizing System 2, the department anticipated potential cost savings, including decreased hardware and software licensing costs and

[6] At the time, Education was part of the Department of Health, Education, and Welfare.

[7] COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading information technology research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language. See Gartner, *IT Market Clock for Application Development*, August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

decreased costs associated with changes to business rules. According to the agency, other potential benefits of modernizing this system included integration across the enterprise, improved cybersecurity and data protection, reduced system complexity, and improved system efficiency.

Department of Health and Human Services—Indian Health Service

Reported number of users: Approximately [illegible]

Initial year of implementation: [illegible]

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: [illegible] million

Reported annual labor costs: [illegible] million

Reported cost of modernization: Agency had not calculated

Potential cost savings: Agency had not calculated

Other benefits: Improved interoperability with other healthcare partners and enhanced patient care

Status of modernization plans: Agency did not have a modernization plan

Source: GAO analysis of agency documentation and interviews as of June 2019. | GAO-21-524T

System 3, as of June 2019

The Department of Health and Human Services' (HHS) System 3 was a clinical and patient administrative information system. HHS's component, Indian Health Service (IHS), used the system to gather, store, and display clinical, administrative, and financial information on patients seen in a clinic, hospital, or remotely through the use of telehealth and home visit practices.

At the time, HHS officials stated that the modernization of System 3 was imperative. Specifically, the agency noted that the system's technical architecture and infrastructure were outdated. This resulted in challenges in developing new capabilities in response to business and regulatory requirements. Further, System 3 was coded in C++ and MUMPS. MUMPS is a programming language that HHS considered to be a legacy language.[8] The agency noted that it had become increasingly difficult to find programmers proficient in writing code for MUMPS. Lastly, the system's more than 50 modules were added over time to address new business requirements. The software was installed on hundreds of separate computers, which led to variations in the configurations at each site. According to IHS, this type of add-on development becomes detrimental over time and eventually requires a complete redesign to improve database design efficiency, process efficiency, workflow integration, and graphical user interfaces.

While as of June 2019, the agency did not yet have modernization plans, in September 2018, HHS awarded a contract to conduct research for modernizing IHS's health information technology (IT) infrastructure, applications, and capabilities. According to the department, the research was to be conducted in several stages, and a substantial part of the research was to be an evaluation of the current state of health IT across IHS's health facilities. Once the research was conducted, in consultation with IHS and its stakeholders, the contractor intended to use the findings and recommendations to propose a prioritized roadmap for modernization. According to HHS, the agency anticipated that it might have been able to begin to execute an implementation plan as early as 2020.

[8] MUMPS was originally known as the Massachusetts General Hospital Utility Multi-Programming System. It is a programming language developed originally for building medical systems. In January 2018, we reported that there is a dwindling supply of qualified software developers for MUMPS.

With regards to potential cost savings, HHS noted that the modernization would take significant capital investment to complete and it was unknown whether the modernization will lead to cost savings. HHS officials stated that this modernization could improve interoperability with its health care partners, the Department of Veterans Affairs and the Department of Defense, and significantly enhance direct patient care.

Department of Homeland Security—Federal Emergency Management Agency

Reported number of users: On average 30,000; more during a disaster

Initial year of implementation: Between 2008 and 2011

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? No

System criticality (as determined by agency): High

System security risk (as determined by agency): High

Reported annual operating costs: $1.2 million

Reported annual labor costs: $0

Reported cost of modernization: Agency had not calculated

Potential cost savings: Agency had not calculated

Other benefits: Ability to meet mission requirements, reduction of network downtime, and increased network availability

Status of modernization plans: Agency had documented modernization plans that described the work necessary to modernize the system; however, they did not contain milestones to complete the modernization or plans for the disposition of legacy system components following system modernization.

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 4, as of June 2019

The Department of Homeland Security—Federal Emergency Management Agency's (FEMA) System 4 consisted of routers, switches, firewalls, and other network appliances (all referred to as devices) to support the connectivity of FEMA sites.

According to the agency, at the time, System 4 needed to be modernized because there were significant cyber and network vulnerability risks associated with its end of life (i.e., no longer supported or manufactured by the vendor) devices. In particular, the system's devices typically require replacement every 3 to 5 years from the date of purchase. Despite this, at the time, the majority of the hardware was purchased between 8 and 11 years ago. As of December 2018, about 545 of these devices were at the end of life.

In a security assessment report performed in September 2018, System 4 received 249 security findings, of which 168 were high or critical risk to the system. Further compounding this issue, the agency was not certain exactly how many devices made up the system. In particular, FEMA officials stated that the vendor completed an inventory of devices in May 2018, but that inventory did not align with other inventory counts. As a result, the agency planned to develop an inventory reconciliation strategy and process to address this issue.

As of June 2019, FEMA intended to replace System 4's devices in two phases. The first phase was planned to target the agency's smaller facilities, while the second phase was planned to address the larger facilities, which may require more complex installations. In 2019, FEMA's Office of the Chief Information Officer was conducting site surveys to better define requirements and cost estimates. While the agency had yet to develop finalized modernization plans for this initiative with milestones, DHS officials and contract information technology staff developed a list of future recommended activities that would help modernize the system as part of their November 2018 quarterly business review. Despite the lack of finalized plans, as of June 2019, FEMA intended to replace 240 of the 545 devices that were at the end of support, if funds were available. The agency also intended to upgrade the remaining 305 devices in the future, if funds were available.

The agency had not calculated the exact amount of cost savings. Once the system was completely updated and a lifecycle replacement operations and maintenance support plan was in place and funded, FEMA and DHS expected to realize cost savings based on new technology and increased throughput.[9] Further, the agency stated that with new equipment, it would be able to meet mission requirements and take advantage of new technologies. In addition, replacing these unsupported devices would significantly reduce downtime and increase network availability.

[9] Throughput refers to the performance of tasks by a computing service or device over a specific period. It measures the amount of completed work against time consumed and may be used to measure the performance of a process, memory, and/or network communications.

Department of the Interior—Bureau of Reclamation

Reported number of users: 40

Initial year of implementation: 2001

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: [illegible]

Reported annual labor costs: [illegible]

Reported cost of modernization: [illegible] million

Potential cost savings: $152,000 per year

Other benefits: Increased capacity for new system requirements, elimination of obsolete hardware, increased system reliability

Status of modernization plans: Agency had documented modernization plans that included milestones to complete the modernization, descriptions of the work necessary to modernize the legacy system, and plans for the disposition of legacy system components following system modernization

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

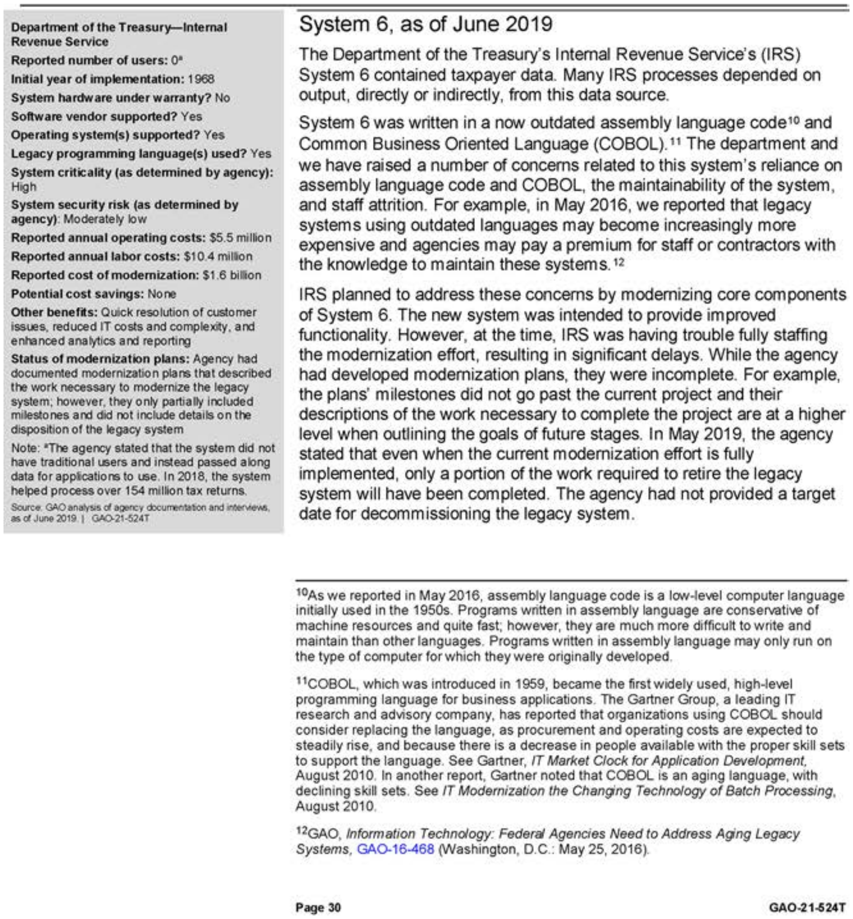
System 5, as of June 2019

The Department of the Interior's (Interior) System 5 was an Industrial Control System (ICS) Supervisory Control and Data Acquisition (SCADA) System that supported the general operation of dams and power plants on a particular river and its tributaries. The system served its customers by, among other things, starting and stopping the generators, adjusting the output of electricity to assure electric grid stability, and monitoring the operating conditions of dam and power plant equipment.

As of June 2019, the system was approximately 18 years old and contained obsolete hardware that was not supported by the manufacturers. Further, according to a program official, the system's original hardware and software installation did not include any long-term vendor support. Thus, any original components that remained operational may have had long-term exposure to security and performance weaknesses. In January 2014, the Director of National Intelligence testified that ICS and SCADA systems used in electrical power distribution provided an enticing target to malicious actors and that, although newer architectures provided flexibility, functionality, and resilience, large segments of the systems remained vulnerable to attack, potentially causing significant economic or human impact. Further, according to Interior's system modernization plans, the agency needed to modernize the system in order to increase data collection capabilities and security. Specifically, the system was expected to interface with more plant equipment and collect and report on more data than it has in the past.

According to Interior's plans, the modernized system was expected to accommodate future growth requirements. The plans also supported the complete replacement of the system's obsolete hardware and software. The modernization plans also outlined goals, milestones, and the work to be accomplished. The agency planned to complete the modernization by January 2020.

By replacing the legacy system, Interior planned to realize a number of potential benefits, including annual cost savings of $152,000. In addition, with modernization, the system would no longer run on obsolete, unsupported hardware. Furthermore, newer software and hardware were expected to allow for the automation of compliance tasks, increase system security, and expand system availability. According to the system's fiscal year 2017 operational analysis, these benefits should create a more reliable system for both the agency and the customers of the networked hydroelectric dams.



Department of the Treasury—Internal Revenue Service

Reported number of users: 0[a]

Initial year of implementation: 1968

System hardware under warranty? No

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately low

Reported annual operating costs: $5.5 million

Reported annual labor costs: $10.4 million

Reported cost of modernization: $1.6 billion

Potential cost savings: None

Other benefits: Quick resolution of customer issues, reduced IT costs and complexity, and enhanced analytics and reporting

Status of modernization plans: Agency had documented modernization plans that described the work necessary to modernize the legacy system; however, they only partially included milestones and did not include details on the disposition of the legacy system

Note: [a]The agency stated that the system did not have traditional users and instead passed along data for applications to use. In 2018, the system helped process over 154 million tax returns.

Source: GAO analysis of agency documentation and interviews, as of June 2019. | GAO-21-524T

System 6, as of June 2019

The Department of the Treasury's Internal Revenue Service's (IRS) System 6 contained taxpayer data. Many IRS processes depended on output, directly or indirectly, from this data source.

System 6 was written in a now outdated assembly language code[10] and Common Business Oriented Language (COBOL).[11] The department and we have raised a number of concerns related to this system's reliance on assembly language code and COBOL, the maintainability of the system, and staff attrition. For example, in May 2016, we reported that legacy systems using outdated languages may become increasingly more expensive and agencies may pay a premium for staff or contractors with the knowledge to maintain these systems.[12]

IRS planned to address these concerns by modernizing core components of System 6. The new system was intended to provide improved functionality. However, at the time, IRS was having trouble fully staffing the modernization effort, resulting in significant delays. While the agency had developed modernization plans, they were incomplete. For example, the plans' milestones did not go past the current project and their descriptions of the work necessary to complete the project are at a higher level when outlining the goals of future stages. In May 2019, the agency stated that even when the current modernization effort is fully implemented, only a portion of the work required to retire the legacy system will have been completed. The agency had not provided a target date for decommissioning the legacy system.

[10] As we reported in May 2016, assembly language code is a low-level computer language initially used in the 1950s. Programs written in assembly language are conservative of machine resources and quite fast; however, they are much more difficult to write and maintain than other languages. Programs written in assembly language may only run on the type of computer for which they were originally developed.

[11] COBOL, which was introduced in 1959, became the first widely used, high-level programming language for business applications. The Gartner Group, a leading IT research and advisory company, has reported that organizations using COBOL should consider replacing the language, as procurement and operating costs are expected to steadily rise, and because there is a decrease in people available with the proper skill sets to support the language. See Gartner, *IT Market Clock for Application Development*, August 2010. In another report, Gartner noted that COBOL is an aging language, with declining skill sets. See *IT Modernization the Changing Technology of Batch Processing*, August 2010.

[12] GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, D.C.: May 25, 2016).

While IRS did not anticipate cost savings associated with the modernization of this system, it anticipated many internal and external benefits for both the taxpayer and the agency. In particular, according to the IRS's *Fiscal Year 2019 Capital Investment Plan*, the benefits of modernizing this system included: (1) increased agility of agency response to changing taxpayer priorities and legislation; (2) reduced IT costs and complexity; (3) enhanced analytics and reporting to greatly improve compliance and issue resolution; and (4) reduced burden of manually intensive processes on IRS employees, by enabling automated calculations that currently were not possible.

Department of Transportation—Federal Aviation Administration

Reported number of users: [illegible]

Initial year of implementation: 1984

System hardware under warranty? Unknown

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? No

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: [illegible] million

Reported annual labor costs: [illegible] million

Reported cost of modernization: Agency had not calculated

Potential cost savings: Agency had not calculated

Other benefits: Enhanced security, compliance with law

Status of modernization plans: Agency did not have a modernization plan

Source: GAO analysis of agency documentation and interviews as of June 2019. | GAO-21-524T

System 7, as of June 2019

The Department of Transportation's (Transportation) Federal Aviation Administration's (FAA) System 7 contained information on aircraft and pilots. The system also provided information to other government agencies, including those responsible for homeland security and investigations of aviation accidents.

According to Transportation, the system was DOS-based and needed to be updated to continue to efficiently meet its mission.[13] Specifically, some of the core system components were mainframe applications that had been in operation since 1984. In addition, the system was running unsupported software, including one operating system that was last supported by the vendor in 2010.

As of June 2019, FAA was planning to implement a new system to streamline processes, allow for the submission of electronic applications and forms, automate registration processes, improve data availability, and implement additional security controls. However, the agency did not have a documented modernization plan. At the time, officials stated that the agency was seeking alternatives to modernize the system and meet legislative requirements. FAA had asked interested vendors to respond to a request for information. According to the agency, the responses to this request were intended to inform strategic decisions about the modernization, and are planned to ultimately lead to proposed solutions from industry.

While FAA had not calculated the specific cost savings associated with modernizing the system, the agency stated that it anticipated potential cost savings. Agency officials stated that they planned to have information on the anticipated cost savings in November 2019. The agency also expected that the modernized system would provide enhanced security.

[13] DOS, originally known as a disk operating system, is the operating system of a computer that can be stored on and run off of a computer disk drive.

Office of Personnel Management

Reported number of users: Millions of external users and [illegible] internal users

Initial year of implementation: [illegible]

System hardware under warranty? Yes

Software vendor supported? No

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately low

Reported annual operating costs: $[illegible] million

Reported annual labor costs: $[illegible] million

Reported cost of modernization: Approximately $[illegible] million

Potential cost savings: Approximately $[illegible] million in cost avoidance in fiscal year 2018

Other benefits: Reduction in cybersecurity and operational risks, ability to address security vulnerabilities, avoidance of operational disruptions

Status of modernization plans: Agency had documented modernization plans that partially included milestones to complete the modernization and partially described the work necessary to modernize the legacy system; however, they did not include plans for the disposition of legacy system components following system modernization.

Source: GAO analysis of agency documentation and interviews. | GAO-21-524T

System 8, as of June 2019

The Office of Personnel Management's (OPM) System 8 consisted of the hardware, software, and service components that supported OPM's information technology (IT) applications and services. This system supported the agency's business functions and supported the agency in providing investigative products and services for more than 100 federal agencies.

Modernizing this system was especially important due to past security incidents and persistent security concerns. Specifically, according to OPM, segments of the agency's infrastructure were allowed to age beyond end of life and posed a significant risk in performance and security to IT operations.[14] Further, in October 2017, OPM's Office of the Inspector General (OIG) reported that the agency's IT environment contained many instances of unsupported software and hardware, where the vendor no longer provided patches, security fixes, or updates for the software. As a result, the OIG noted that there was increased risk that OPM's IT environment contained known vulnerabilities that would never be patched, and could have been exploited to allow unauthorized access to data. In June 2015, OPM reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate but related incident had compromised its systems and the files related to background investigations for 21.5 million individuals. At a June 2015 Congressional hearing, OPM's Director stated that the modernization of the IT infrastructure was critical to protecting the agency's data from adversaries. The Director also stated that it was not feasible to implement encryption on networks that were too old, but noted that OPM was taking other steps to secure the networks.[15]

At the time, OPM planned to modernize System 8 by upgrading hardware at the end of life, migrating off of legacy operating systems and support software, and augmenting the agency's established policies and procedures. In fiscal year 2018, OPM completed software and hardware upgrades, including replacement of core switches, network end points, and laptops. In fiscal year 2019, the agency planned to continue its focus

[14] OPM, *Congressional Budget Justification and Annual Performance Plan, Fiscal Year 2019*, (Washington, D.C.: February 2018).

[15] *OPM: Data Breach, Hearing Before the House Committee on Oversight and Government Reform*, 114th Cong. (statement of Director of the Office of Personnel Management Katherine Archuleta).

on refreshing aged IT infrastructure, so that its hardware components will have the proper vendor support. OPM developed multiple documents related to the planning of this modernization effort, including a modernization schedule, and its fiscal year 2019 budget justification.

However, the modernization plans contained in these documents did not include details for the entire modernization effort. The milestones in these documents, for instance, were either no longer current or only contained milestones regarding one part of the project. While the budget justification outlined what it planned to accomplish in fiscal years 2018 and 2019, it did not mention the rest of the work needed to complete the infrastructure modernization.

Similarly, the OIG had reported concerns regarding the agency's plans to modernize its infrastructure.[16] In June 2018, the OIG reported that OPM was generally continuing in the right direction toward modernizing its IT environment, but the OIG had concerns with the agency's plan for modernization and its overall approach to IT modernization. For example, the OIG was concerned that OPM's planning documents did not identify the full scope of the modernization effort or contain cost estimates for the individual initiatives or the effort as a whole. The OIG planned to monitor and continue to report on the agency's progress in modernizing its infrastructure.

OPM anticipated realizing both financial and nonfinancial benefits with the modernization of its infrastructure. For example, as a part of its overall infrastructure modernization, the agency avoided approximately $16 million in costs as part of its data center consolidation efforts for fiscal year 2018. The agency also expected that cybersecurity and operational risks associated with end of life hardware would be reduced. To that end, the agency stated that remediating end of life hardware also should allow OPM the ability to address identified security vulnerabilities and avoid operational downtime, as support became more readily available.

[16] See, for example: OPM Office of the Inspector General, Office of Audits, *Management Advisory: U.S. Office of Personnel Management's Fiscal Year 2017 IT Modernization Expenditure Plan*, Report Number 4A-CI-00-18-022 (Feb. 15, 2018) and *Final Management Advisory: U.S. Office of Personnel Management's Fiscal Year 2018 IT Modernization Expenditure Plan*, Report Number 4A-CI-00-18-044 (June 20, 2018).

Small Business Administration

Reported number of users: Approximately [illegible]

Initial year of implementation: 2002

System hardware under warranty? No

Software vendor supported? No

Operating system(s) supported? No

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderately high

Reported annual operating costs: [illegible]

Reported annual labor costs: [illegible]

Reported cost of modernization: [illegible]

Potential cost savings: None

Other benefits: Increased security and stability of the system

Status of modernization plans: Agency had a documented modernization plan that included milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, it did not include a description of the work necessary to complete the modernization.

Source: GAO analysis of agency documentation and interviews as of June 2019. | GAO-21-524T

System 9, as of June 2019

The Small Business Administration's (SBA) System 9 was a system that, according to the agency, provided identification, authentication, and authorization services[17] for several of the agency's applications.

According to the agency, the system was developed by SBA and originally implemented in 2002. At the time, agency officials stated that System 9's hardware and software were no longer supported by the associated vendors. Consequently, according to the agency, it was paying for extended support contracts that had increased operating costs for the system. Further, agency officials stated that the system resided on a platform that was scheduled to be decommissioned within the year. In addition, the system was coded using a programing language that the agency considered to be a legacy programming language (among others).

As of June 2019, the agency's documented modernization plan included milestones to complete the modernization and plans for the disposition of the legacy system following system modernization; however, the plan did not include a description of the work necessary to complete the modernization. However, agency officials stated that it intended to replace the system's functionality with login.gov. Login.gov was developed and is maintained by the General Services Administration as a single sign-on trusted identity platform.[18] Login.gov provides identification and authentication for applications and is intended to offer the public secure and private online access to participating government programs. However, according to the agency, since login.gov did not provide authorization controls, SBA intended to develop additional software to provide authorization controls beginning in March 2019.

[17] Agencies design and implement access controls to provide assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals. These controls protect computer resources from unauthorized use, modification, disclosure, and loss by limiting, preventing or detecting inappropriate access to them. Two of these control areas are identification and authentication, and authorization. Identification and authentication controls allow a computer system to identify and authenticate different users so that activities on the system can be linked to specific individuals. Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file.

[18] Single sign-on reduces the burden of multiple passwords. It is intended to increase security of the data and systems and compliance with federal information technology policies and best practices.

As of June 2019, according to the agency, it did not anticipate any cost benefits from modernizing System 9. However, the agency expected that the security and stability of the system would increase.

Social Security Administration

Reported number of users: Over [illegible]

Initial year of implementation: [illegible]

System hardware under warranty? Yes

Software vendor supported? Yes

Operating system(s) supported? Yes

Legacy programming language(s) used? Yes

System criticality (as determined by agency): High

System security risk (as determined by agency): Moderate

Reported annual operating costs: $[illegible] million[a]

Reported annual labor costs: $[illegible] million

Reported cost of modernization: $[illegible] million (from fiscal year [illegible] to [illegible])

Potential cost savings: Approximately $[illegible] million per year from fiscal year [illegible] through fiscal year [illegible][a]

Other benefits: Better access to beneficiary data, faster and more efficient claim processing, reduced need for manual data entry, and fewer number of improper payments, among others.

Status of modernization plans: Agency had documented plans that [illegible] milestones that partially covered the modernization effort and partially described the work necessary to modernize the system; however, they did not contain plans for the disposition of legacy system components following system modernization.

Note: [a]The agency was unable to update the operating costs or potential cost savings for this system. The figures presented are the costs and potential savings for all of the systems operating in the mainframe environment.

Source: GAO analysis of agency documentation and interviews as of June 2019. | GAO-21-524T

System 10, as of June 2019

The Social Security Administration's (SSA) System 10 supported the provision of particular Social Security benefits to eligible people. At the time, SSA collected detailed information from the recipients in person, by telephone, and via the internet on multiple platforms (e.g., desktops and hand-held devices), and from internal and external interface methods. System 10 was comprised of many applications that collected information, made payments, and communicated with SSA's clients.

According to SSA's October 2017 information technology modernization plan, the agency needed to modernize its core systems, including System 10, because of complications related to their age and original system design.[19] SSA's modernization plan indicated that, since implementation, these systems had been subjected to constant modifications to incorporate changes in legislation, regulations, and policy. Through the years, new technologies and capabilities had been integrated into the core systems and delivering new capabilities was becoming exorbitantly expensive.

Further, as of June 2019, most of the agency's systems, including System 10, were generally unconnected to each other, creating functional silos servicing independent lines of business. According to the agency, navigating these systems was challenging, and copying beneficiary data from system to system could result in data becoming out of sync.

According to the agency's modernization plan, SSA intended to replace its core systems, including System 10, with new components and platforms, engineered for usability, interoperability, and future adaptability. Work accomplished over several years of incremental modernization had already resulted in moving a substantial portion of System 10 away from old technologies. For instance, according to SSA officials in the Office of the Deputy Commissioner, Systems, SSA moved System 10 to a modern, relational database platform and modernized aspects of the user interface.[20] According to an SSA 5-year modernization roadmap, the agency was currently working to modernize and create web services as a part of the effort to consolidate SSA's initial

[19] Social Security Administration, *IT Modernization: A Business and IT Journey* (Baltimore, MD: Oct. 2017).

[20] A relational database is a system that allows users to store data in and retrieve data from linked databases that are perceived as a collection of relations or tables.

claims processes; however, the roadmap did not offer specific information about these efforts.

As for its modernization planning efforts, SSA's plans included overall modernization goals, a high-level overview of the planned system architecture, milestones for fiscal year 2018, and a description of the work that it had planned to accomplish in fiscal year 2018. However, the plans did not include either System 10-specific milestones or a description of the work necessary to modernize the legacy system beyond fiscal year 2018. Further, the document did not include plans for the disposition of the legacy system after modernization. According to officials in the Office of the Deputy Commissioner, Systems, the agency intended to update the planning documentation and make further decisions as the modernization effort progressed.

SSA expected that modernizing System 10 would result in cost savings in addition to many other benefits. For instance, the agency expected that it would be able to save approximately $38 million from modernizing System 10 and other systems running in the agency's mainframe environment. In addition, increased staff access to benefit recipients' data would enable staff to review medical evidence faster and process claims more accurately, among other things. According to the agency's modernization plan, the improvements to the system would improve productivity and service to the public, as well as reduce the number of improper payments due to technician error.

Written Testimony of

Casey Coleman
Senior Vice President for Digital Transformation,
Salesforce Global Public Sector

Before the

Emerging Threats and Spending Oversight Subcommittee
of the
Committee on Homeland Security and Governmental Affairs

U.S. Senate

Controlling Federal Legacy IT Costs and Crafting 21st Century IT Management Solutions

April 27, 2021

Written Testimony of

Casey Coleman
Senior Vice President for Digital Transformation,
Salesforce Global Public Sector

Before the

Emerging Threats and Spending Oversight Subcommittee
of the
Committee on Homeland Security and Governmental Affairs

Controlling Federal Legacy IT Costs and Crafting 21st Century IT Management Solutions

April 27, 2021

Good morning Chairman Hassan, Ranking Member Paul, and distinguished members of the subcommittee. Thank you for inviting me to testify today; it is a privilege to discuss federal Information Technology (IT) modernization issues with you. My name is Casey Coleman, and I am the Senior Vice President for Digital Transformation at Salesforce Global Public Sector. I have been in my current role for four years. I previously served for almost twelve years at the U.S. General Services Administration, including six and a half years as the agency's Chief Information Officer (CIO). Additionally, I have served in leadership roles at AT&T Government Solutions and Unisys Federal, and have also held consulting and engineering roles at several technology startups. I began my career as a software engineer with a division of Lockheed Martin. The compilation of those experiences has made me acutely aware of the challenges and opportunities confronting federal IT.

Today's hearing on this important topic is very timely. Modernizing federal IT has been a priority for a long time, but the prospects for progress have been significantly improved with the emergence of modern cloud-based digital platforms. The world's largest banks, manufacturers, healthcare companies and retailers are already transforming their operations and customer service by embracing the cloud. The federal government can do the same.

Over $92 Billion annually is spent on federal IT systems. All functions of government depend on their successful operation, including our nation's defense, public health, service to citizens, economic stability and much more. In an increasingly all-digital world, the demands and expectations on this infrastructure is growing but the government is increasingly unable to meet the demand. The result is a disruption in the public trust and vulnerability to emerging threats such as we have seen with the outbreak of COVID-19.

There are many factors that contribute to the difficulty of modernizing legacy IT systems. These systems often rely on increasingly obsolete technologies and scarce expertise to manage them, so they become brittle and prone to failure. The IT team often is hesitant to make any but the most critical changes for fear of system failure and program outages. Organizational structures and processes are developed to accommodate system limitations, which serves to inhibit innovation. And while the commercial world has moved to mobile and digital services across every industry, these innovations can be difficult and slow for the government to procure. Modern, agile IT practices require different technologies, and design skills that often are in short supply for departments and agencies.

The result is that the government becomes cut off from the rapid evolution of commercial and consumer innovation. Most importantly, the situation creates a very vulnerable cybersecurity situation. Our IT systems are under constant attack and yet we are always playing catch up, not taking advantage of best in class commercial platforms that are constantly upgraded and hardened.

Despite these challenges, there are many notable modernization success stories. I'm especially passionate about this because I've seen it firsthand. As the CIO for GSA through much of the Bush 43 and Obama Administrations, I had the privilege of leading a multi-year modernization program to move GSA to the cloud, improve security, and improve service delivery for our employees and customers.

Our first step was to consolidate all infrastructure, from 40 different contracts and 15 helpdesks, into a single agency-wide program. We cut costs by 30% and improved security patching from over a month to near real time. We modernized employee tools and remote access so that employees could work from anywhere and be closer to their customers. GSA was the first agency to migrate to cloud platforms, and we developed the FedRAMP cloud cybersecurity program. We also moved to a zero-baseline budget, so that we could understand the incumbent costs, and identify targets for modernization and cost-cutting with greater effectiveness.

When the Obama Administration announced the Cloud First policy, we led the way, becoming the first to move the entire agency to cloud platforms (Google Apps and Salesforce) for email, collaboration, productivity and low-code rapid application development tools.

Our previous system was on really old hardware. We didn't know when it went down. I used to send myself emails at night and on weekends just so I would know if it was still working. By making this shift, all of our employees had critical systems available anytime, anywhere, on any device. We vastly improved our cybersecurity and records management, and the investment paid for itself in a year. But more importantly, we were better at our mission and more resilient. When weather emergencies like the Snowmageddon and SuperStorm Sandy hit the East Coast a few years ago, all federal offices were shut down but GSA kept right on going, working remotely. This resiliency has continued to serve them well even through the pandemic.

Why does this matter? In addition to improvements in cybersecurity, resiliency, records management and cost savings, we were *much more agile*. Modernization cannot be a once-and-done effort, or it will fade in effectiveness as the world evolves. Rather, by embracing commercial cloud platforms GSA was able to leverage commercial innovation and securely deploy new services, fast, when new demands arose.

This success story is far from unique. In 2020, we saw many governments respond almost overnight to COVID-19 challenges, rolling out digital services for contact tracing, quarantine management, unemployment claims, emergency benefits, vaccine management, and much more. We saw years of modernization compressed into a few months. These initiatives weren't on anyone's radar before the pandemic, but things that once took months or years were done in days or weeks.

What made the difference? Moving to the cloud. This rapid pace of response was enabled by innovative digital cloud platforms — commercially-delivered solutions, providing secure, prebuilt components that are nimble enough to accommodate both private and public sector needs. The primary benefit for government agencies is that it allows them to participate in an ecosystem that is regularly updated and constantly evolving to keep pace.

Why does it matter? For a Farmer, they can get their crop loan through a mobile app, get seed in the ground, and not waste a day off the tractor. For a Veteran, seeing their doctor by video means they continue to receive the treatment they need and the benefits they've earned. For all citizens, better experiences with government mean greater public trust.

And this pivot is important for government employees. No one comes into the government to step backward in time and do their work the hard way, with brittle old tools that were state of the art decades ago. They want to serve a mission, make a difference, give back. If we want to recruit and retain talented public servants who could choose to go elsewhere, we have to give them the tools that empower them and make their work effective and rewarding.

To summarize, modern cloud technology platforms are a complete game changer for improving government service delivery and mission execution. I do not mean to suggest that this is a silver bullet, and I have included recommended reforms[1] for procurement, operations and budgeting in the Recommendations below, which I am glad to discuss further. But all of those other factors only click when you add the cloud.

In closing, technology modernization is absolutely essential in order to ensure the federal government is able to deliver its critical missions for the good of our nation. I am confident that this is achievable and have observed first-hand what can be achieved, and the trust dividend that successful modernization delivers. Thank you to the Subcommittee for your focus on this vital matter and I look forward to more detailed conversations.

[1] A thoughtful summary of recommended reforms can be found at https://alliance4digitalinnovation.org/, in the downloadable PDF report "Priorities for the Incoming Administration and Congress," December 2020

I would like to respectfully submit the following suggestions for federal IT modernization:

1. Fix the Way the Government Acquires and Uses Technology Solutions. The Federal government's response to the COVID-19 pandemic has shown what is possible when exigent circumstances arise and immediate challenges require innovative thinking and new technology operating models. Going forward, agencies should build on the bright spots that have surfaced during this difficult time and powerfully embrace disruption in all aspects of the technology, security, and IT acquisition. To ensure this change is lasting, the 117th Congress can pursue legislation that would repeal numerous outdated Federal IT laws (such as Clinger-Cohen and the E-Government Act of 2002) and in their place create a new, comprehensive foundation for Federal IT operations, management, acquisition, and oversight.[2]
2. We are encouraged to see the increased funding for the Technology Modernization Fund (TMF) and participated in a multi-association letter recommending reforms to help departments and agencies take full advantage of this significant opportunity[3]. These reforms include improved project selection, more robust program office staffing, and expanded repayment options. Additionally, I believe that prioritizing projects that utilize digital cloud platforms will result in the best and most lasting outcomes.
3. Technology modernization and management agenda recommendations to the new Administration were published by ACT-IAC, an educational nonprofit that brings government and industry together. I participated in the committee that developed the recommendations and would commend these to the Subcommittee as a framework that supports IT modernization.[4] Notably, we suggest the creation of an "Agile First" policy, similar to the Cloud First policy of

[2] More details of this recommendation can be found at https://alliance4digitalinnovation.org/, in the downloadable PDF report "Priorities for the Incoming Administration and Congress," December 2020

[3] https://alliance4digitalinnovation.org/wp-content/uploads/2021/03/Letter-to-OMB-and-GSA-on-TMF-Implementation_03-24-2021.pdf

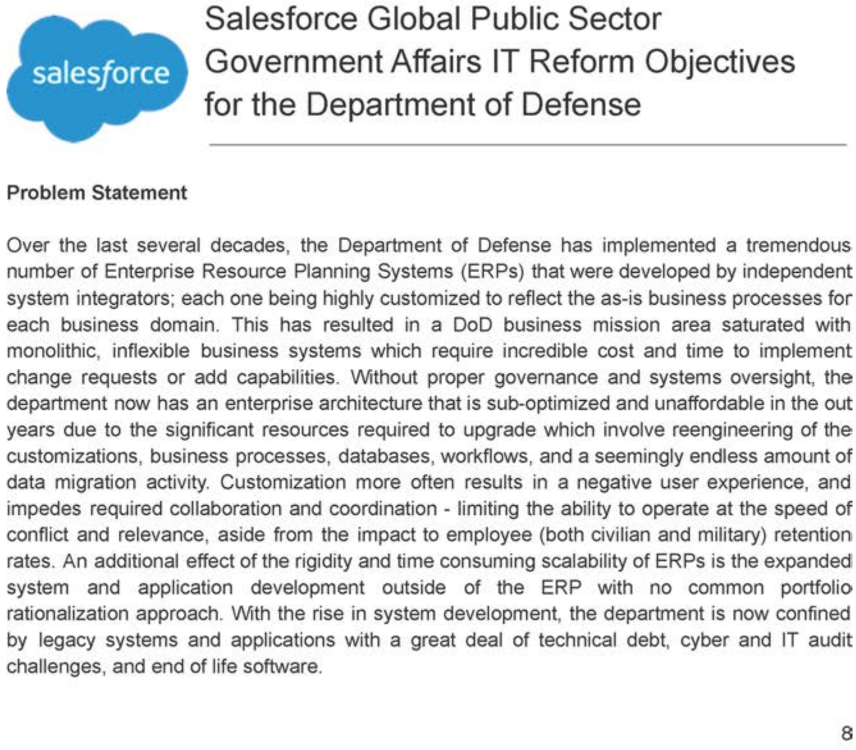
[4] https://www.actiac.org/content-page/agenda-2021-presidential-election-project

the Obama Administration, to update the government's policy and process foundation to match the focus on modern IT.

4. Our team and I would be delighted to visit with Subcommittee Members and staff to share more details of government modernization successes and challenges, to help with greater context and understanding.

ADDENDUM

As a final observation, one of the most complex and costly IT challenges for the federal government is its multitude of Enterprise Resource Planning (ERP) systems. Salesforce has developed a white paper on a way forward for the government and especially for the Department of Defense. We would like to submit this as an attachment for consideration by the Subcommittee.



salesforce

Salesforce Global Public Sector Government Affairs IT Reform Objectives for the Department of Defense

Problem Statement

Over the last several decades, the Department of Defense has implemented a tremendous number of Enterprise Resource Planning Systems (ERPs) that were developed by independent system integrators; each one being highly customized to reflect the as-is business processes for each business domain. This has resulted in a DoD business mission area saturated with monolithic, inflexible business systems which require incredible cost and time to implement change requests or add capabilities. Without proper governance and systems oversight, the department now has an enterprise architecture that is sub-optimized and unaffordable in the out years due to the significant resources required to upgrade which involve reengineering of the customizations, business processes, databases, workflows, and a seemingly endless amount of data migration activity. Customization more often results in a negative user experience, and impedes required collaboration and coordination - limiting the ability to operate at the speed of conflict and relevance, aside from the impact to employee (both civilian and military) retention rates. An additional effect of the rigidity and time consuming scalability of ERPs is the expanded system and application development outside of the ERP with no common portfolio rationalization approach. With the rise in system development, the department is now confined by legacy systems and applications with a great deal of technical debt, cyber and IT audit challenges, and end of life software.

In our dynamic environment, it is critical that the DoD's business systems represent the best of the commercial private sector, and allow for timely, accurate, and secure data for decision making.

Recommendation

Through a collaborative and transparent set of discussions and meetings with the Professional Staff and the Members, Salesforce would recommend that the US Congress - the committees of jurisdiction for the Department of Defense - engage one another to ensure future IT solutions are as military as necessary, and as commercial as possible. As mentioned by Senator Jack Reed, Chairman of the Senate Armed Services Committee, at the Emerging Technologies and Their Impact on National Security hearing on 23 February 2021, "*We need to make sure we are looking at the right technologies, have the processes in place to take advantage of them and to deliver new capabilities to war fighters at the speed of technological change. Overlaying this is the competition with China in both the national security and economic sectors.*"

We believe that the DoD needs to change the way it looks at software development and acquisition, as well as the underlying technology to avoid perpetuation of an environment that consistently eats away at the services O&M appropriation by creating technical debt. This can be solved by forming a committee of private sector professionals and government experts to provide a report on how to reform the DoDI 5000.75 - Business Capability Acquisition Cycle to provide for the ability to quickly acquire best-in-class technology such as SaaS and PaaS solutions. We also believe that the Department of Defense is predisposed to acquiring monolithic ERPs and customizing the modules to fit as-is business processes, vice utilizing a SaaS solution to digitally transform enterprise operations by providing a Post-Modern ERP solution that puts the Service Member at the center of every transaction. This post-modern ERP and multi-cloud approach provides fit for purpose architecture that enforces speed, agility, transparency, and mobile solutions.

Solutions

We are eager to see the Department continue to work on implementing these innovative practices and measures and believe additional steps would improve the Department's ability to access the most innovate, secure software available to support the Business Mission Area with speed, agility to provide rapid deployment of capabilities and incremental improvements:

- **Reform the Business Capability Acquisition Lifecycle (DoD 5000.75)**: DoD should embrace agile software development, incremental delivery, cloud migration, Software as a Service adoption, and Human Centered Design User Experience. DoD has often experienced cost overruns and schedule delays to defense business system investments, while delivering capabilities that no longer align to the current need and requirement of business leaders. BCAC was implemented inefficiently and modified by many in the department to a series of waterfall, milestone driven steps that hamper any opportunity to implement with speed and agility. The committee should mandate that current and future business domains be assessed as a fit for purpose Platform as a Service (PaaS) or Software as a Service (SaaS) solution with current or emerging platforms. The committee should enforce and mandate the use of PaaS or SaaS and require a justification be presented otherwise.

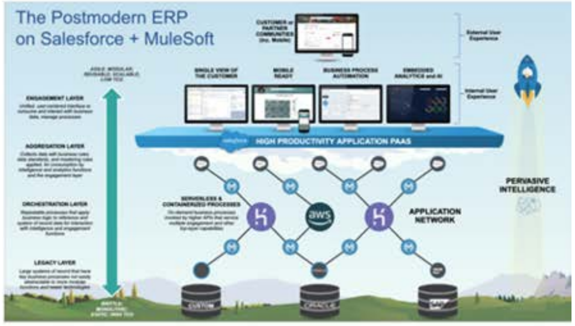
- **Embrace best-in-class commercial solutions**: DoD continues to maintain and sustain a business domain portfolio of primarily antiquated, legacy systems and applications with cyber security vulnerabilities, technical debt, out of date and unsupported software and hardware, and financial audit findings. To alleviate this grave situation across the entire department, the single path to Enterprise Resource Planning (ERP) solutions will not work as we have seen over the past two decades. DoD must take a leap to current technology through digital transformation and not ERP modernization alone. ERP modernization is a must and should be the priority of the department to reduce, consolidate and focus on core functionality of the ERP (HR core, FM General Ledger, Logistics). The committee should mandate and enforce compliance of digital transformation and a future state architecture of multi-cloud solutions complementing the ERP. Multi-cloud solutions allow efficiency, speed and agility to deliver and scale with Software as a Service solutions that are secure, scalable and available. This platform approach to portfolio management greatly reduces the complexities of the legacy environment, reduces the system inventory and challenges, increases capacity and capability and enforces improved warfighter readiness.

- **Embrace Business Process Automation (BPA), Business Process Reengineering (BPR) and Workflow Automation through the adoption and utilization of SaaS:** DoD is plagued with manual, repetitive and redundant business processes across the business mission area. These antiquated processes deliver untimely and out of date business services to all servicemembers and their families – the DoD's top priority should be best practices and services to the warfighter and families. The lack of business process automation makes any department wide business service standardization impossible as we have seen over the many years and attempts to design and deliver joint solutions. With the adoption of SaaS, the services and agencies can reimagine business processes and workflows in a completely automated, transparent and efficient manner. The committee should mandate the establishment of a business reform council and governance body within OSD that evaluates the services and agencies in the adoption of business reform that enforces business process automation, standardization and a community of practice across the department to share best practices and streamline services delivered to warfighters and their families globally.

- **Human Centered Design and Mobile**: DoD has often experienced a poor user experience through the lack of focus in designing services and solutions that are personalized like servicemembers' personal lives. Historically, the user experience or user interface has been an afterthought when fielding business systems and applications. The committee should mandate the use of Human Centered design principles in the ideation phase of new solutions to meet current and emerging needs. The committee should manage compliance through the reformed BCAC process to require user input, ethnography and incorporation of modern user interfaces, consistently found in SaaS platforms. Further, the committee should mandate a mobile strategy across the department and track service and agency progress toward fielding business solutions and services that offer mobile apps without the use of the Common Access Card. There are many emerging Identify, Credentially, and Access Management tools in the Gov Cloud marketplace that offer multi-factor authentication.

- **Planning, Programming, Budgeting, Execution (PPBE) Reform***:* The Department of Defense utilizes a decades old governance model and process for the building of the Program Objective Memorandum, and its Budget. The Senate Armed Services Committee should require a report on how this process could be modernized and optimized along with an implementation plan. The current PPBE system does not allow for agility when responding to fact of life changes in defense and national security strategy, and requirements can take 2+ years to reach the President's Budget submission. To move at the speed of relevance and implement modern technology that will enable our ability to maintain overmatch with our peer adversaries, a thorough review of the entire PPBE process is overdue.

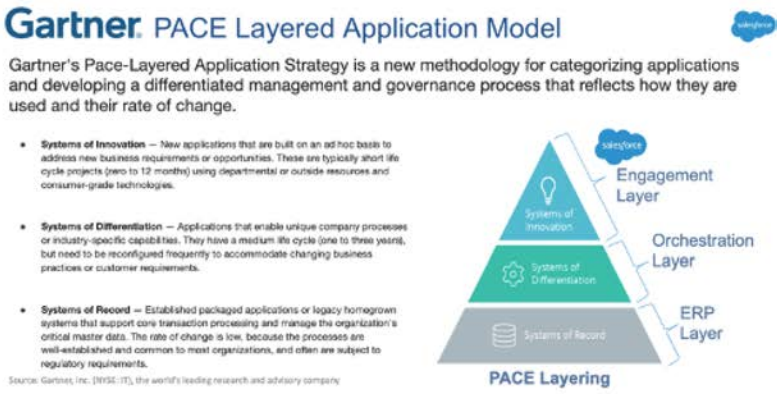
- **Post Modern ERP:** We recommend that the DoD adopt a new approach, which Gartner characterizes as "Postmodern ERP Enterprise" ensuring the existing DoD ERPs, and their feeder systems, are integrated with an agile SaaS/PaaS platform, like Salesforce, in an effort to orchestrate new systems (both on premise and cloud) to create a new "System of Service Member Engagement."



Salesforce proposes the DoD assess all the thousands of existing scripted and coded customizations in the ERP environments that are causing massive ERP upgrade issues and determine which defense business processes are logical candidates to be moved to the agile Salesforce PaaS platform, thus relegating ERP back to its core functionality. This would reduce the complexity and cost of the current DoD ERP environment, and result in an agile, low-code/no-code solution to solve challenges quickly and affordably. Further, Salesforce proposed the DoD evaluate the business mission area domain and plethora of legacy systems that can easily be roadmapped to the Salesforce platform and sunset/decommissioned.

The key to streamlining the process without sacrificing the user experience is to separate the user interaction layer from the transactional data hub. When you provide a powerful user layer (Customer Relationship Management or "CRM" solution) for your processes everyone benefits by having a 360-degree view into its customers (the Service Member), the users and all interactions, automating the business life-cycle processes, and collaborating with the stakeholders in a single user experience. Transactional records can be stored in the on-prem ERP, but made visible in Salesforce through our flexible data integration options. This can be configured easily and quickly through rapid application development and be based on current use cases and data guidelines.

We believe that using separate platforms for these functions would facilitate a significantly improved user experience, improve data quality, increase agility, and significantly lower costs. Please refer to the following diagram and our recommendations for Salesforce as the user layer.



Gartner. PACE Layered Application Model

Gartner's Pace-Layered Application Strategy is a new methodology for categorizing applications and developing a differentiated management and governance process that reflects how they are used and their rate of change.

- **Systems of Innovation** – New applications that are built on an ad hoc basis to address new business requirements or opportunities. These are typically short life cycle projects (zero to 12 months) using departmental or outside resources and consumer-grade technologies.

- **Systems of Differentiation** – Applications that enable unique company processes or industry-specific capabilities. They have a medium life cycle (one to three years), but need to be reconfigured frequently to accommodate changing business practices or customer requirements.

- **Systems of Record** – Established packaged applications or legacy homegrown systems that support core transaction processing and manage the organization's critical master data. The rate of change is low, because the processes are well-established and common to most organizations, and often are subject to regulatory requirements.

Source: Gartner, Inc. (NYSE: IT), the world's leading research and advisory company

Conclusion

These recommendations support congressional interest in expanding and solidifying the use of agile software development methodologies, cloud infrastructure hosting, SaaS adoption, and a focus on streamlined/modern business processes and services supporting servicemembers and their families. Further, these recommendations will drive three major outcomes: transformed, personalized user experience, significantly enhanced business process and workflow automation, and system and application rationalization. By pursuing the recommendations outlined above, the DoD can achieve digital transformation and a common business services model across the department, meeting efficiency and effectiveness goals while preserving the precious resources appropriated to the department and providing for a “back office business function” that supports our ability to maintain overmatch with our near-peer adversaries.

Testimony of Renee P. Wynn

Former Chief Information Officer of the National Aeronautics and Space Administration

FOR A HEARING ON

Controlling Federal Legacy IT Costs and

Crafting 21st Century IT Management Solutions

BEFORE THE

United States Senate

Homeland Security and Governmental Affairs Committee Subcommittee on Emerging Threats and Spending Oversight

April 27, 2021

Washington, D.C.

Good morning Chairwoman Hassan, Ranking Member Paul, and distinguished members of the Subcommittee. I am honored to testify today on the importance of Information Technology (IT) modernization, highlighting barriers and challenges in the IT modernization process and how Congress and agencies can work together to address them.

Now is an ideal time for departments and agencies to begin or continue large, complex IT modernization projects. Much has been learned about remote working and delivering federal government services during the COVID pandemic. This learning can be used to accelerate modernization efforts. To do this, the departments and agencies must have the right personnel, processes, and budgets in place to significantly increase the probability that such IT modernization projects will be successful.

As the former Chief Information Officer (CIO) of NASA and the Acting CIO and Deputy CIO of the Environmental Protection Agency (EPA), I have had ample opportunity to understand the dynamics inherent in modernizing federal government IT. My experience as NASA's (CIO) gave me the best view of the biggest challenge a CIO faces when modernizing IT in the federal government - an agency's culture, which is sometimes referred to as the "people challenge." A CIO must have sustained support and funding for IT modernization from the Agency heads to her executive management team, she must have the right people with the right skills, including the contractor workforce, and build and maintain relationships across the Agency and with the contractor community. Without this support, complex IT projects will fail.

NASA's Business Service Assessment

Prior to my arrival, NASA had initiated and completed a Business Services Assessment (BSA). The BSA was undertaken to identify organizational and management improvement areas for NASA's mission support services. This included, but was not limited to, procurement, facilities, and human resources. IT was the first mission support function assessed, and the findings resulted in a list of recommendations. Some key recommendations covered revising the governance process to include mission executives and non-IT executives from the different NASA centers, establishing more enterprise-wide IT services, better software management practices and the need for an improved cybersecurity program.

The CIO office developed and executed an implementation plan based on the BSA recommendations. While implementing the plan, my team and I learned many valuable lessons. We adjusted our approach based on our experiences and highlighted an issue that was preventing us from gaining the full benefit of the BSA recommendations and future IT modernization efforts: too much of NASA's IT budget and staff (civil servants plus contractors) were not managed by the NASA CIO. This made it difficult for NASA to control IT spending because many of the geographically dispersed Centers were independently establishing IT service contracts or buying software, even though the CIO office provided the service or had existing software licenses available. Misalignment of budget and organization plagued the other mission support areas already implementing their BSA recommendations, too.

NASA used insights from the BSA to create a Mission Support Future Architecture Plan (MAP) to make holistic improvements across the entire mission support operations spectrum. MAP took the bold and politically charged step of having all the people and budget associated with a mission support function report to the head of the mission support function, such as the Chief Human Capital Officer (CHCO), the Chief Procurement Officer (CPO), or the CIO. The two largest mission support functions, IT and Facilities, were scheduled to be the two final organizations to go through the MAP process. This allowed the agency to learn from implementing MAP before starting on the largest, most complex organizations.

As I led the transformation resulting from the BSA and MAP, I found the most significant challenge was addressing culture, again this is sometimes referred to as the "people challenges." As I saw it, people challenges can be divided into three categories – those that worked for me (including contractors); those that worked for the other mission support functions; and those that I served, the civil servants and contractors delivering NASA's complex mission.

The people, civil servants, and contractors, that worked for me were extremely talented, but concerned that the BSA meant they were not valued by NASA and were seen as doing a poor job. To this end, I and the Center CIOs spent a lot of time reassuring them that NASA did value them, and the BSA was a gift that elevated the importance of their work and increased their value to NASA.

The other mission support areas were frequently critical of the CIO and IT modernization projects. While the Chief Financial Officer (CFO), Chief Human Capital Officer (CHCO) and Chief Procurement Officer (CPO) understood the need for MAP for their area, there was resistance from some of them because they faced losing their IT staffs to the CIO. This resistance affected our collaboration efforts. I and my Deputy had to work to regain the trust we needed for mutual success and future IT modernization projects.

NASA's top executives provided steadfast support of the NASA CIO throughout the mission support transformational efforts. However, the executives and staff below them were resistant and at times, difficult. Nothing rattles a civil servant more than having portions of their budgets and staff reallocated. When difficulties would arise, either I, my Deputy or a Center CIO would have to work with them to address their concerns. We were not always successful at soothing hurt feelings, but many a painful conversation would at least result in better mutual understanding, and improved working relationships. To say the least, my team and I spent a lot of time working culture change or the "people challenges."

Congressional Support

Congress has taken appropriate steps to address IT management and cybersecurity risks through legislation. From the Clinger-Cohen Act of 1996 to the Federal Information Security Modernization Act of 2014 (FISMA) and to the Federal Information Technology Acquisition and Reform Act of 2015 (FITARA), all were designed to advance government services to the public and provide improved information security for the U.S. government. The legislation gave the CIO the authorities to lead the way for more modern and secure IT so the public would be better served.

With the passage of the Modernizing Government Technology (MGT) Act, Congress continued its support to improve Federal technology by providing financial resources to agencies through the creation of a central modernization fund housed by the General Services Administration (GSA). These funds are allocated through the Technology Modernization Fund (TMF) board. The board's primary objectives lie in evaluating project proposals submitted by agencies wishing to use some portion of the TMF as well as monitoring the progress of the funded IT modernization projects.

The oversight of Congress has also been a driving factor in making the intended improvements. This needs to continue as a bipartisan, unified approach, as it has had a positive impact on how seriously past administrations have focused on IT modernization and cybersecurity. These legislative actions plus sustained oversight, have provided the foundation to improve IT management and cybersecurity for the federal government.

Congressional action taken over the years has given the federal government a solid foundation for pursuing IT modernization so the government can better serve the public.

Going Forward

I have learned during my tenure as the NASA CIO that successful IT modernization projects require sustained and predictable budgets, the right people, and unwavering internal leadership support to deliver their expected benefits.

Congress should remain focused on IT modernization and cybersecurity through oversight hearings, providing predictable appropriated budgets and funding for the TMF. Oversight hearings with the CIO should also include other Department or Agency leadership such as, but not limited to, the Chief Procurement Officer, Chief Financial Officer and even the Chief Human Capital Officer. Together, they should provide the update on large, complex IT modernization projects. Finally, Congress should also be prepared to act should gaps emerge in the federal government's ability to deliver more modern and effective public services.

The CIO must also have the right workforce, an appropriate blend of civil servants and contractors invested in the mission of the federal government. Yet, the federal government continues to struggle with recruiting and retaining experienced IT professionals, especially those with the skills to run large IT projects. Contractors help fill the gap, but there needs to be a blend of civil servants and contractors working on every IT project. There is no specific ratio, just an effective balance. It is an art and depends upon the complexity of the IT project. Current civil servants must have time to keep up to date on technology advances, as well participate in re-skilling opportunities. Early efforts to re-skill existing federal employees have been successful. This should continue. Whether a civil servant or a contractor, all involved must have the knowledge, skills, and expertise to meet the growing demands of IT modernization and cybersecurity.

Internal to agencies, department and agency heads should provide unwavering support for IT modernization and cybersecurity projects so the CIO can address the culture, IT workforce and budget challenges.

IT modernization and improved cybersecurity practices are fundamental requirements for delivering improved and secure federal services to the American public.

Thank you for the opportunity to appear before the Subcommittee today and testify on this critical topic. I stand ready to answer your questions.

Written Testimony of Max Everett
Former Chief Information Officer (2017–2020)
at the U.S. Department of Energy

Before the Emerging Threats and Spending Oversight Subcommittee
of the Committee on Homeland Security and Governmental Affairs

April 27, 2021

Chairwoman Hassan, Ranking Member Paul, and Members of the Committee, thank you for the opportunity to speak on this important subject.

I have spent almost two decades in and around Federal IT, both as a Federal appointee and a contractor. I hope to candidly share what I have observed in that time.

The events of the last year have illuminated how truly critical dealing with legacy IT is for the effective operation of government. Dealing with the need to allow our Federal workforce to work remotely, providing efficient access to government services to all Americans impacted by COVID, and protecting our systems from recent serious cybersecurity attacks have all put this subject front and center.

I would begin by suggesting that we must be broad in our view of what constitutes legacy IT. It is not only those obvious systems that have passed their end of life – whether they are mainframes or unsupported software. It includes cobbled together systems like paper-based forms or outdated front-end websites that prevent customers – citizens – from finding what they need quickly and effectively.

One way to measure the value of our systems is data. We can look no further than the Federal government's efforts to combat COVID over the last year to understand the importance of data. Data helps us measure effectiveness and predict where resources should go to have the greatest impact. Yet some of the most valuable data the Federal government has continues to be locked up in our legacy systems, and often on paper.

During my tenure as Chief Information Officer (CIO) at the Department of Energy (DOE), we began focusing on the move to electronic document management to improve service delivery for citizens and liberate data from paper that was often merely filed away in a drawer or warehouse. I have been encouraged to see that effort continuing at across government under the path put forward by the 21st Century IDEA Act.

As we discuss the road from legacy systems to IT modernization, we must focus on sustainable and continuous innovation. One of the most straight forward ways we can talk about this challenge is in the two categories of people and process.

The people problem in Federal IT is significant. Our current human capital system is simply ill-prepared to meet the demands for recruiting, re-training, and retaining IT professionals of all kinds. The current channels for recruiting are not effective in reaching new and broader pools of candidates. Our job descriptions are often outdated and focused on irrelevant qualifications for the needs at hand.

As CIO at the Department of Energy, I often faced significant challenges exercising the expanded hiring authorities that I had on paper. The private sector offers more money and often more engaging workplaces. I believe we should continue to seek new paths for Departments and Agencies to be creative in bringing new technology talent into their ranks.

The good news here is that we have existing options. Progress has been made on greater hiring authorities for technology roles, but those need to be enforced and communicated across the Federal Human Capital community. The recent increase in funding for the US Digital Service will bring an influx of skilled technologists who can make an immediate impact.

Growing the number of digital focused internships and fellowships also provides an opportunity to let future leaders in the technology community see some of the unique challenges they can address in Federal government. Who else can offer an immediate opportunity to positively impact every American?

Contractors are also an incredibly important part of the staffing for IT across the Federal government. Technology contractors typically outnumber their Federal employee counterparts by three or four to one and sometimes even more. Contractors offer the ability to quickly onboard staff with new skills or access specific technical skills sets for short periods of time. I believe it is very important to keep our reliance on contractors in mind when discussing IT staffing solutions.

At DOE, we moved our primary IT services contract to a managed services model. This simply means we provide business requirements to our contractor and ask them to use their experience and capabilities to provide a result. This moves us out of the realm of micromanaging contractors that has failed time and again across government.

Process is a broader issue and one that I believe Congress can assist with by continuing to demand adherence to the laws already in place.

I am a biased observer, but I believe CIO authorities are critical to the success of modernization. I was fortunate to have the support of the Secretary and Deputy Secretary while I was at DOE. In fact, our Department moved into compliance with FITARA as soon as I joined when my reporting structure was moved to the Secretary and Deputy Secretary. Several agencies followed our lead afterwards.

That reporting structure and access allowed me to understand the priorities of the Department and engage other senior leaders as peers in conversations on budgeting and cybersecurity risk management.

Turning to other existing tools, the Modernizing Government Technology (MGT) Act can play a critical role in supporting accelerated modernization across Federal government.

The Department of Energy received one of the first Technology Modernization Fund (TMF) awards in 2018, something I take great pride in. I was incredibly encouraged that Congress provided $1 billion dollars to the TMF fund. That level of funding shows that Congress has prioritized modernization in a way that expects measurable results.

I would note that TMF is not simply about the money. TMF represents a methodology for managing IT and modernization. To receive a TMF award, the agency must demonstrate an understanding of their total cost of ownership for systems and show the numbers. That is a fundamental change in how technology is managed in the Federal government, in my experience.

One of the challenges we have seen in TMF projects is that the repayment requirement makes it very difficult to use for much needed projects that improve citizen and customer experience on websites and public-facing systems. It is notoriously hard to quantify cost savings for those type of systems.

With that in mind, I am supportive of suspending or waiving repayment of the TMF funds, but ONLY if the process is followed. The rigor in reporting and oversight that TMF brings Federal IT is, to me, just as critical as the dollars.

A second element that is less often discussed in the MGT Act is the IT working capital fund. Establishing these funds has been hamstrung at many Departments, but I believe they are invaluable to CIOs. Managing IT in the Federal government is already challenging, but most CIOs must spend an inordinate amount of time dealing with "color of money" issues. Single year money that must be spent by the end of a fiscal year is a recipe for incentivizing bad decisions.

Most major government systems are capital expenditures (CapEx). A large amount of money is spent over a set time to build the systems. The spending moves to operations and maintenance – O&M. An unfortunate process then begins in which we often run that system until it is already at the end of life before someone realizes it needs a radical update or replacement. Those costs necessary to modernize the systems accrue over time in what we call technical debt.

If the organization has single year funding, there are few options for saving over time to fund modernization of those larger systems. One is asking for a large appropriation for the new system, all too often without any analysis of how the previous system performed, or any type of cost benefit analysis. The second option is that a clever Federal manager might be able to put money aside in various ways if they have access to multi-year money or other funding mechanisms. The most common option is simply robbing Peter to pay Paul. Forced by necessity, other services or systems are cut to fund the updated system.

There are a few ways to improve this situation. The first is establishment and funding of Technology Working Capital Funds as envisioned in the MGT Act. This will allow Departments to fund larger modernization projects over time in a formal and visible way.

The second is moving to operational expenditure (OpEx) focused models – Software as a Service (SaaS) and cloud solutions. This is a less discussed value of using cloud solutions, but it allows for better management and projection of costs over time while building in the cost of upgrades and enhancements.

I will finally briefly mention cybersecurity, which is obviously top of mind for all of us in the IT community given the attacks on our systems over the last few months.

Modernizing our IT systems is a clear critical step in protecting the Federal enterprise. Cyber defenders already face significant challenges against dedicated nation state adversaries, but the odds against them become overwhelming when attempting to defend out of date and un-patched systems.

Our old models under FISMA, measuring cybersecurity over the course of months and years, is woefully inadequate. We have depended on compliance frameworks that are not focused on risk far too often. Most organizations simply do not have the time to keep up with all the cybersecurity checklists they are asked to fill out, and so we have far too many people focused on that rather than the fundamental work of managing risk in real time. We must move to models for continuous monitoring of systems, which will require data and visibility at network speed.

Programs like FedRAMP need additional resources and must speed up so that we can bring innovative new solutions to the Federal market faster. Architectures like zero trust must be evolved and become the standards for additional defense in depth of our Federal networks.

My experience has been one of seeing slow and steady progress in these areas over the years, but our need for rapid progress has never been greater. As budgets increase for our technical needs, it becomes ever more important that we evolve and improve how we manage Federal technology.

I believe continuing the improvements embodied in legislation like FITARA and the MGT Act will make it easier to recruit some of the best and brightest innovators to become CIOs and digital leaders in Federal government. Many have given up substantial income in the private sector to join government out of a desire to serve, only to encounter bureaucratic processes that prevent them from making a real impact.

These changes will also have a direct impact on improving our Federal cybersecurity posture. Modernized systems will be more manageable and defendable for our cybersecurity teams across government.

Thank you again for inviting me here today. I look forward to answering your questions.

Questions for the Record
Senate Homeland Security and Governmental Affairs:
Emerging Threats and Spending Oversight Subcommittee
Controlling Federal Legacy IT Costs and Crafting 21st Century Management Solutions
Tuesday, April 27, 2021
Senator Kyrsten Sinema

Questions for Mr. Kevin Walsh

1. **Based off of your research into the 10 most critical Federal information technology legacy systems (as reported in GAO-19-471), what are a few key elements that must be part of a successful IT modernization plan, and what steps need to be taken by the Administration and Congress, respectively, to ensure they are included?**

   As we reported in June 2019, agencies should have documented modernization plans for legacy systems that, at a minimum, include three key elements: (1) milestones to complete the modernization, (2) a description of the work necessary to modernize the legacy system, and (3) details regarding the disposition of the legacy system.[1] Without complete legacy system modernization plans that include these elements, agencies' modernization initiatives will have an increased likelihood of cost overruns, schedule delays, and overall project failure.

   In addition, to help ensure the successful modernization of federal legacy systems, in May 2016 we recommended that the Office of Management and Budget (OMB) direct agencies to identify legacy systems needing to be replaced or modernized.[2] At that time, we reported that agencies may not be effectively planning for the modernization of legacy systems, in part, because they were not required to. Specifically, agencies were not required to identify, evaluate, and prioritize existing information technology (IT) investments to determine whether they should be kept as-is, modernized, replaced, or retired.

   As of June 2021, OMB had not implemented our recommendation. In responding to the recommendation, OMB staff stated that agencies were directed to manage the risk to High Value Assets,[3] which can include legacy systems, in OMB's

[1] GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems,* GAO-19-471 (Washington, D.C.: June 11, 2019).

[2] GAO, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems,* GAO-16-468 (Washington, D.C.: May 25, 2016).

[3] According to OMB's December 2018 guidance, an agency may designate federal information or an information system as a High Value Asset when one or more of these categories apply to it: (1) the information or information system that processes, stores, or transmits the information is of high value to the federal government or its adversaries; (2) the agency that owns the information or information system cannot accomplish its primary mission-essential functions within expected timelines without the

December 2018 guidance.[4] However, while OMB's guidance does direct agencies to identify, report, assess, and remediate issues associated with High Value Assets, it does not require agencies to do so for all legacy systems. Until OMB requires agencies to identify all of their legacy systems that need to be replaced or modernized, the federal government will continue to run the risk of maintaining investments that have outlived their effectiveness.

For its part, Congress has enacted important legislation—the provisions commonly referred to as the Modernizing Government Technology (MGT) Act—to help further agencies' efforts to modernize IT.[5] Congress' continued oversight will be vital to ensuring that agencies successfully plan for, and carry out the modernization of, their critical legacy systems.

2. **As we consider steps needed to modernize Federal IT, what are your recommended changes to the Modernizing Government Technology (MGT) Act and/or the Technology Modernization Fund to help ensure more effective use and oversight of the fund?**

To help ensure more effective use and oversight of the Technology Modernization Fund (TMF), OMB and the General Services Administration (GSA) should implement our prior recommendations on the fund. In December 2019, we reported that OMB and GSA's TMF Program Management Office were experiencing challenges in estimating the cost savings of the funded modernization projects and were likely to face further challenges in recovering expenses associated with operating the fund in a timely manner. [6] As a result, we recommended that OMB and GSA develop and implement a plan to fully recover the program's operating expenses, and that GSA develop guidance to assist agencies in creating cost estimates for modernization projects. OMB and GSA have not yet implemented these recommendations. To ensure the effective use and oversight of the fund, it will be important for them to do so.

In addition, on March 11, 2021, Congress and the President enacted the *American Rescue Plan Act of 2021* that appropriated an additional $1 billion to be available until September 30, 2025, to carry out the purposes of the fund.[7] Further, in May 2021, OMB and GSA announced an updated model for distributing funds from the TMF that focused on prioritization and flexibility with repayment of the funds. This increase in funding, coupled with the announced changes to the TMF fund distribution model, also underscores the need for OMB

information or information system; and (3) the information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

[4] OMB, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

[5] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, Div. A, Title X, Subtitle G, 131 Stat. 1283, 1586-94 (2017).

[6] GAO, *Technology Modernization Fund: OMB and GSA Need to Improve Fee Collection and Clarify Cost Estimating Guidance for Awarded Projects,* GAO-20-3 (Washington, D.C.: Dec. 12, 2019).

[7] American Rescue Plan Act of 2021, Pub. L. No: 117-2, Title IV, § 4011, 135 Stat. 4, 80 (2021).

and GSA to implement our recommendations to ensure the appropriate oversight of how these increased funds are awarded and used.

Further, Congress may want to consider the challenges that OMB has reported in implementing the MGT Act. In addition to creating the TMF, the MGT Act provides authorization for all agencies covered by the Chief Financial Officers Act of 1990[8] to establish IT working capital funds.[9] Our work has not examined this specific area; however, in its February 2018 guidance on implementing the MGT Act, OMB stated that the act does not confer transfer authority and, therefore, agencies may only transfer funds to the working capital funds if they have other authority that authorizes the transfer of such funds.[10] While several agencies have received authority to make transfers into working capital funds, still others have noted that they lack the authority to make transfers into IT working capital funds. Congress may want to consider how to enhance agencies' authorities to use these working capital funds.

3. **What other actions should Congress prioritize to ensure federal agencies can improve IT acquisitions and operations and strengthen federal cybersecurity measures?**

Congress may want to prioritize providing continued attention and oversight to federal agencies' efforts to improve IT acquisitions and operations and strengthen federal cybersecurity—two critical areas highlighted in our high-risk series. We testified in April 2021[11] that Congressional action has aided progress in (1) building the federal government's capacity (i.e., people and resources) for better managing IT acquisitions and operations and (2) establishing an office responsible for, among other things, improving the coordination of cybersecurity policy and operations across the executive branch.[12] Congress' continued oversight will be vital to ensuring that agencies' actions to improve IT acquisitions and operations and strengthen federal cybersecurity are sustained.

[8] The 24 major federal agencies covered by the Chief Financial Officers Act of 1990 are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and U.S. Agency for International Development. 31 U.S.C. § 90l(b).

[9] Working capital funds provide a mechanism for agencies to centralize and simplify the funding and provision of shared services within and between federal agencies. It is a self-sustaining fund that collects fees from agency customers to pay for services financed through the account.

[10] OMB, *Implementation of the Modernizing Government Technology Act*, M-18-12 (Washington, D.C.: Feb. 27, 2018).

[11] GAO, *Information Technology and Cybersecurity: Significant Attention Is Needed to Address High-Risk Areas,* GAO-21-422T (Washington, D.C.: Apr. 16, 2021).

[12] Section 1752 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021), established, within the Executive Office of the President, the Office of the National Cyber Director.

Our March 2021 update to our high-risk series stressed that significant attention was needed to address challenges related to improving the federal government's management of IT acquisitions and operations.[13] We noted in our update that overall progress in addressing this area has remained unchanged since our prior high-risk report in 2019. We have continued to emphasize that OMB and other federal agencies need to continue to fully implement critical requirements of the statutory provisions commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA).[14] In addition, in the March 2021 update, we reported that OMB has continued to demonstrate its leadership commitment by issuing guidance to agencies to implement FITARA. We also noted that it will be important for OMB to maintain this current level of leadership and commitment to further ensure that agencies succeed. To this end, sustained executive branch and congressional attention will remain essential to ensuring progress in addressing long-standing IT management challenges.

With regard to strengthening federal cybersecurity, and in light of recent cybersecurity attacks, Congress's continued oversight of federal agencies' efforts to address urgent cybersecurity risks will also be essential. In the March 2021 high-risk report, we reiterated the importance of agencies taking 10 critical actions to address four major cybersecurity challenges facing the nation: (1) establishing a comprehensive cybersecurity strategy and performing effective oversight, (2) securing federal systems and information, (3) protecting cyber critical infrastructure, and (4) protecting privacy and sensitive data.[15] These 10 critical actions are to:

- develop and execute a more comprehensive federal strategy for national cybersecurity and global cyberspace;
- mitigate global supply chain risks (e.g., installation of malicious software or hardware);
- address cybersecurity workforce management challenges;
- ensure the security of emerging technologies (e.g., artificial intelligence and Internet of Things);
- improve implementation of government-wide cybersecurity initiatives;
- address weaknesses in federal information security programs;
- enhance the federal response to cyber incidents;
- strengthen the federal role in protecting the cybersecurity of critical infrastructure (e.g., electricity grid and telecommunications networks);
- improve federal efforts to protect privacy and sensitive data; and
- appropriately limit the collection and use of personal information and ensure that it is obtained with appropriate knowledge or consent.

[13] *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[14] *Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

[15] GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges,* GAO-21-288 (Washington, D.C.: Mar. 24, 2021).

In May 2021, to address persistent and increasingly sophisticated cyberattacks, the President issued Executive Order 14028, *Improving the Nation's Cybersecurity*.[16] This executive order identifies a range of key cybersecurity efforts for agency action, such as developing plans to implement Zero Trust Architecture[17] and updating contracting requirements and language to require prompt sharing of information related to cyber threats and incidents. As outlined by the executive order, agencies will have to take several immediate actions to ensure stronger cybersecurity across their enterprise. Congress' continuing oversight of agencies' efforts to address the critical actions recommended by GAO and required by the executive order should help to better position the nation to prevent, or more quickly detect and mitigate the damage of, future cyberattacks.

[16] The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[17] Zero Trust Architecture is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

Questions for the Record
Senate Homeland Security and Governmental Affairs
Emerging Threats and Spending Oversight Subcommittee
"Controlling Federal Legacy IT Costs and Crafting 21st Century Management Solutions"
Tuesday, April 27, 2021
Senator Kyrsten Sinema
Questions for Ms. Casey Coleman

1. There continues to be Federal agencies resisting the adoption of digital cloud-based platforms. What are the benefits and risks associated with using these platforms to secure government data and do the benefits outweigh the risks?

Thank you for your interest in this important topic and for providing me an opportunity to lend my expertise to expediting the digital transformation of federal IT systems. I am aware of some limited resistance to IT modernization efforts in specific instances in the federal government. In these rare cases, fear of disruption or of new costs is used as a rationale for the status quo.

The reality is that any comprehensive analysis would show that, generally, the long-term costs of maintaining bespoke legacy IT systems - including specialized personnel and cumbersome patching processes - far exceeds any short-term costs incurred to acquire and implement modern solutions. That is to say nothing of the immediate improvements to user experience, cross-organization functionality, mobile capabilities, audit, and cybersecurity that come with adopting the cloud. In today's world, it is also important to acknowledge that when a system moves to the cloud, any discovered vulnerabilities are addressed with consistent, automatic, and timely updates.

My years working alongside many talented government employees has convinced me that most federal IT professionals believe in their mission. They are open to utilizing new tools that can maximize their efficacy and would prefer to work with the cutting edge, private sector standard. Funding and some reforms will, of course, be required to support these individuals but, critically, leadership is also needed to empower government IT workers. Projects should be designed to use agile methods and deliver rapid incremental progress, within an organizational culture that allows for learning and revisions to be made over time. If we can craft policies that increase access to commercial solutions and allow CIOs to demonstrate leadership in implementation, we will be taking important steps toward more effectively harnessing the many benefits that recent advancements in technology can provide throughout federal agencies.

2. What steps can be taken to encourage buy-in to these cloud-based systems and what role can Congress play to move towards broader adoption of these systems across Federal agencies?

<u>Oversight</u>
In holding this hearing, the members of the Subcommittee have already taken an important step uniquely available to Congress. The federal bureaucracy is vast and inefficiencies tend to

proliferate in the shadows. I encourage the Subcommittee, and other Members of Congress, to continue vigilant oversight on the topic of federal IT modernization. It truly is a policy space where enormous gains can be made on behalf of American taxpayers and to strengthen institutions. Furthermore, IT has become so critical to all government functions that accountability should be expected at the highest levels of all departments and agencies, not just at the CIO level.

Funding

Beyond the many functional enhancements available through digital transformation, realizing lifetime operational cost savings is an attractive benefit. However, it will take near-term investment to ensure federal agencies can get on the path to modernization and future savings. That is why leaders from several industries are asking Congress to fully fund the president's budget request of $500 million for the Technology Modernization Fund in fiscal year 2022. Recent reforms to the program should help those dollars more quickly reach agencies ready to execute IT modernization strategies.

Reforms

- Unfortunately, it is not common for federal agencies to have a comprehensive reference of all products and services provided by the agency; nor will they have a comprehensive view of those provided by other similar or relevant agencies. Congress should advance policies that encourage all departments and agencies to catalogue their programs and services that meet public needs in a transparent and consistent fashion, with a view towards proactive evaluation of processes that can be streamlined, expedited, or removed as barriers to providing effective services.
- Congress should encourage agencies to develop and publish IT modernization plans, including budget requests, for a defined set of legacy systems.
- Congress should advance policies that encourage the use of commercially available solutions. One place to start would be delivering acquisition guidance that mandates agencies perform effective market research and prioritize commercial procurement options where available.
- Congress should ensure clear authority for agencies to create working capital funds as envisioned in the Modernizing Government Technology Act of 2017.

Questions for the Record
Senate Homeland Security and Governmental Affairs:
Emerging Threats and Spending Oversight Subcommittee
Controlling Federal Legacy IT Costs and Crafting 21st Century Management Solutions
Tuesday, April 27, 2021
Senator Kyrsten Sinema
Questions for Ms. Renee Wynn

1. Even before the recent events with Solarwind and the Microsoft Exchange Server attacks, we knew the importance of mitigating supply chain risks. In December 2020, GAO reported that few of the civilian federal agencies it reviewed had implemented foundational practices for managing information and communication technology supply chain risks. What steps do the Administration and Congress, respectively, need to take to ensure that agency Chief Information Officers incorporate supply chain risks into their planning?

   The first step to success is to continue to recognize that cybersecurity threats in hardware and software supply chains are a threat to national security. No hardware or software, including sensors, operational technology and internet of things items, should be used in a production environment by any federal agency without a cybersecurity supply chain risk management evaluation.

   Based upon (1) the General Accountability Office (GAO) report, December 2020 Supply Chain Risk Management report, and the previous Department of Defense version and (2) the recent Executive Orders on Supply Chain and Cybersecurity, the physical and cyber or digital supply chain risk evaluation work should be merged into one process. We live in an interconnected environment and thus our risk evaluation and management processes should reflect this.

   Some specific actions for consideration:
   1) Assign responsibility to the Federal Chief Information Officers (CIOs) to establish and oversee the Information Communication Technologies (ICT) Supply Chain Risk Management Activities.
   2) Modify existing audit and accountability processes associated with the Federal Information Security Modernization Act and the Federal Information Technology Acquisition Reform Act to include Supply Chain Risk Management, including the current scorecards.
   3) Task heads of agencies to develop an agency-wide ICT Supply Chain Risk Management strategy to include, but not limited to, meeting the GAO Audit findings and document or establish Agency-wide supply chain processes.
   4) Ensure funding is available for each Agency's program.
   5) To ensure cost effective implementation and information sharing across the federal government and with the private sector:
      a. Assign Cybersecurity & Infrastructure Security Agency (CISA) with oversight of the government-wide Supply Chain Risk Management

Questions for the Record
Senate Homeland Security and Governmental Affairs:
Emerging Threats and Spending Oversight Subcommittee
Controlling Federal Legacy IT Costs and Crafting 21st Century Management Solutions
Tuesday, April 27, 2021
Senator Kyrsten Sinema
Questions for Ms. Renee Wynn

program that includes both the physical supply chain as well as the cyber/digital supply chain.

b. In partnership with CISA, assign General Services Administration (GSA) the responsibility of (1) acquiring the tools, (2) training and (3) information sharing needed to support the government-wide Supply Chain Risk Management program.

2. During your testimony, you talked about the success of the Cyber Reskilling Program run by OMB and how it demonstrated when given the chance, the Federal workforce can be reskilled to fill critical workforce needs. What lessons did OMB learn during the planning and execution of this reskilling program that can inform future reskilling programs across the Federal agencies?

   The reskilling project was a success at re-training a small cohort of capable federal employees ready to shift into cybersecurity positions. Future efforts should be expanded to include at least 50 or more employees per cohort and include the identification of cyber positions for cohort graduates.

3. What actions should Congress take to ensure agencies are conducting workforce planning and as part of that planning, developing, and utilizing reskilling programs as they identify needs for IT expertise?

   Congress should continue to focus on this issue and designate a lead agency to work in partnership with academic institutions as well as public-private organizations to formalize the re-skilling program. By designating a lead agency, OPM, DHS, or even GSA, someone will become accountable for action in this area. The lead agency should develop the program using the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NICE Framework) and in consultation with OMB, Federal CIO and Chief Human Capital Officer, to use the lessons learned from the Federal CIO reskilling academy.

   The NICE Framework is the blueprint to categorize, organize, and describe cybersecurity work. It was developed in partnership with the National Initiative for Cybersecurity Education (NICE), the Office of the Secretary of Defense, and Department of Homeland Security (DHS) to provide educators, students, employers, employees, training providers, and policy makers with a systematic and consistent way to organize the way we think and talk about cybersecurity work, and to identify the knowledge, skills, and abilities needed to perform cybersecurity tasks. (Link: NICE Cybersecurity Workforce Framework | National Initiative for Cybersecurity Careers and Studies (cisa.gov))

Congress should request an annual report on the State of Federal IT with a section dedicated to IT Workforce, including the Reskilling Academy. Sufficient qualitative and quantitative data must be included. Suggested metrics should include, but not limited to, number of applications, number of applications accepted, number of students, number of students who successfully completed the program and the number of students placed in cybersecurity positions. The build the program using the Federal CIO Council model as well as the lessons learned. Congress should ask for an annual report to include, but not limited to, number of program participants, participant diversity (e.g., grade, gender, race, location), number of successful program completion and placement of graduates in cybersecurity jobs.

Questions for the Record
Senate Homeland Security and Governmental Affairs:
Emerging Threats and Spending Oversight Subcommittee
"Controlling Federal Legacy IT Costs and Crafting 21st Century Management Solutions"
Tuesday, April 27, 2021
Senator Kyrsten Sinema
Questions for Mr. Max Everett

1. **As we consider steps needed to modernize Federal IT, what are your recommended changes to the Modernizing Government Technology (MGT) Act and/or the Technology Modernization Fund to help ensure more effective use aud oversight of the fund?**

   Congress recent increase in funding of the TMF fund and the newly introduced flexibility in repayment are major improvements and will allow for rapid improvements in citizen-facing legacy systems.

   I would recommend three elements to improve the effective use and oversight of the TMF funds.

   First, and perhaps most importantly, Congress should take whatever legislative steps are necessary to ensure that all Departments and Agencies have an IT-focused Working Capital Fund. This is critical to the mature management of IT and making sustained progress in modernizing government systems. No organization of any kind can expect to make sustained progress or manage system life cycles in a consistent manner under the annual budget and appropriation system in use in most Departments today. The working capital funds would provide the flexibility and responsiveness necessary to support the speed of innovation our taxpayers deserve, as well as allowing for multi-year planning and implementation needed for the largest and most complex Federal IT systems.

   Congress should also request updates on metrics and evaluation of the impact of the newly funded systems on improved services, on a least an annual basis. Beyond cost and schedule oversight, these metrics of the actual impact of updated systems can better demonstrate value to those who remain skeptical.

   Third, Congress should consider establishing an advisory council of public and private sector technology experts to provide further oversight, advice, and evaluation of the TMF program and progress on implementation of the goals of MGT. This council should be distinct from the TMF program office, GSA, and OMB. The council's goal should be to provide all parties, including Congress, feedback and recommendations.

2. **What other actions should Congress prioritize to ensure federal agencies can improve IT acquisitions and operations and strengthen federal cybersecurity measures?**

My first recommendation would be to continue oversight and potentially enhance existing FITARA legislation. FITARA provides valuable authority and oversight to Federal CIOs when exercised appropriately.

Unfortunately, there are still several reasons that FITARA has not matched the promise of that legislation.

Many CIOs lack the staffing necessary to fully evaluate all of the acquisitions across their Departments. Additionally, many procurements are still being awarded without FITARA approval across the Federal government. In some cases, this is due to legacy systems that do not properly identify and code acquisitions that include technology spending; in other cases, there are attempts to directly circumvent FITARA and CIO oversight.

Without that oversight, the Federal government will continue to waste money on obsolete systems or make IT purchases that are not aligned to broader IT life cycle and cybersecurity planning.

To address these issues, several steps are required that will involve offices across government.

At the Department of Energy, my office had a collaborative relationship with the Chief Procurement Officer, and we worked together to increase our visibility into all IT spend across the Department. These relationships between CIOs and CPOs must be encouraged and expanded.

CIO offices need further support for their hiring authorities, and in some cases additional staffing of procurement and project management professionals to better evaluate the volume of IT-related acquisitions. This will requirement not only funding, but OPM and Chief Human Capital Officers to become more agile and responsive.

These additional Federal personnel are critical because far too many Federal offices rely on contract support for sensitive budget and procurement activities. Some Federal offices have contractors with access to financial and procurement planning information while contractors from the same company provide program delivery and bid on contracts. This creates enormous opportunities and incentives for poor contract outcomes. Conflict of interest policies alone are simply not enough to protect from inappropriate sharing of information in those situations.

Additionally, Congress should ensure through continued oversight or language in authorizations and appropriations that all contracts with IT-related expenditures must comply with FITARA.

Finally, Federal CIOs must collaboratively develop and communicate broad enterprise architectures and life cycle requirements for their Departments. This proactive guidance allows program offices and procurement staff to ensure that the solutions they pursue will meet FITARA guidance.

○