UNLOCKING GOVERNMENT EFFICIENCY THROUGH IT MODERNIZATION

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

APRIL 29, 2025

Serial No. 119–23

Printed for the use of the Committee on Oversight and Government Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE
60–197 PDF WASHINGTON : 2025

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
PAT FALLON, Texas
BYRON DONALDS, Florida
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
ELI CRANE, Arizona
BRIAN JACK, Georgia
JOHN MCGUIRE, Virginia
BRANDON GILL, Texas

GERALD E. CONNOLLY, Virginia, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
EMILY RANDALL, Washington
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona
WESLEY BELL, Missouri
LATEEFAH SIMON, California
DAVE MIN, California
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JAMES RUST, Deputy Staff Director
MITCH BENZINE, General Counsel
LAUREN LOMBARDO, Deputy Policy Director
RAJ BHARWANI, Senior Professional Staff Member
DUNCAN WRIGHT, Senior Professional Staff Member
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JAMIE SMITH, Minority Staff Director
CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

LAUREN BOEBERT, Colorado
ANNA PAULINA LUNA, Florida
ERIC BURLISON, Missouri
ELI CRANE, Arizona
JOHN MCGUIRE, Virginia
Vacancy

SHONTEL BROWN, Ohio, *Ranking Minority Member*
RO KHANNA, California
SUHAS SUBRAMANYAM, Virginia
YASSAMIN ANSARI, Arizona

C O N T E N T S

WITNESSES

INDEX OF DOCUMENTS

* No additional documents were submitted for this hearing.

ADDITIONAL DOCUMENTS

UNLOCKING GOVERNMENT EFFICIENCY THROUGH IT MODERNIZATION

Tuesday, April 29, 2025

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

The Subcommittee met, pursuant to notice, at 2:23 p.m., in room 2247, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Burlison, McGuire, Brown, Subramanyam, and Ansari.

Ms. MACE. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will come to order. And welcome, everyone. Without objection, the Chair may declare a recess at any time, and I recognize myself for the purpose of making an opening statement.

Good afternoon and thank you for joining us for this discussion on Federal IT modernization. An important role of this Subcommittee is to ensure proper management of Federal technology. The Trump Administration and the U.S. DOGE service and their efforts to make the government more efficient have prioritized modernizing government technology because they have rightly identified Federal IT as the backbone for all government programs, operations, and, of course, spending.

Federal IT systems enable everything the government does from the national defense and Homeland Security to the administration of benefit programs. And when these systems are outdated, obsolete, and unreliable, the government cannot carry out these duties responsibly or efficiently. The Federal government spends more than $100 billion annually on IT systems, with almost 80 percent of the spending going toward operating and maintaining them, including many legacy systems. These legacy systems which were built on unsupported software or hardware and rely on outdated data centers or coding languages, such as COBOL, a language I learned 25 years ago, plus create dangerous security and operational environments and are costly to maintain.

A few years ago, GAO compiled a list of the 10 Federal IT systems most in need of overhaul due to criticality and their obsolescence. One is a COBOL-based system used to process about 20 mil-

lion Federal student financial aid applications annually. The system is older than the Department of Education, which opened its doors in 1980. I learned COBOL early in my career because coding provides a pathway for girls and women to advance into STEM fields. I actually taught myself to code.

But today's aspiring coders are not learning COBOL. That is why on his first day in office, President Trump signed Executive Order 14158 titled, "Establishing and Implementing the President's Department of Government Efficiency." This Executive Order established DOGE through a reorganization of what was formally known as the U.S. Digital Service, an entity this Subcommittee has collaborated with on a bipartisan basis for many years to promote IT modernization.

The Trump Executive Order includes a requirement for the U.S. DOGE service to work with agency heads to promote interoperability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization. This directive prioritizes efforts aligned with long-time industry best practices and expert recommendations for IT modernization. It also elevates the work USDS has been doing across the three previous administrations under Presidents Obama, Trump, and Biden.

Today, we are here to celebrate the progress that has been made to modernize government technology, review the approaches that have worked, and discuss how the current Trump administration and the renewed USDS can aggressively prioritize proven solutions so we can finally make real progress in building efficient and effective Federal IT.

To this end, we are joined by three of the most senior technology leaders from the first Trump Administration. Ms. Kent, Ms. Graves, and Ms. Roat, you served at the beginning of the COVID–19 pandemic and helped oversee the start of the Federal government shift to remote work. During this time, you learned a lot of processes were also paper based and arcane that could not be carried out digitally, which is a wild and crazy fact that this was happening.

The lack of resiliency in government operations created drastic consequences for our constituents who could not connect with government offices to receive benefits or file required paperwork.

I am looking forward to hearing from you all today about what you learned during this unique time in your government service. It is my understanding this is your first time all testifying together on the same panel. Thanks for being here today.

Speaking of proven solutions, during the Trump Administration, the Modernizing Government Technology Act of 2017 was signed into law. This Act established the Technology Modernization Fund, or TMF, which creates a unique funding vehicle that can be used to improve, retire, or replace Federal IT systems. The TMF is a necessary piece of IT modernization puzzle. Without it, the unpredictability and the annual budget cycle would make it too difficult for some modernization projects to get off the ground.

Last week, I reintroduced the Modernizing Government Technology Reform Act alongside Oversight Committee Ranking Member Gerry Connolly. This bill reforms and reauthorizes the TMF so

that it can continue to be used to assist with IT modernization initiatives moving forward.

With that, I recognize Ranking Member Brown for her opening statement.

Ms. BROWN. Thank you, Chairwoman Mace, for holding this important hearing.

The Federal government has long been behind the curve in modernizing its IT systems. We can all agree on the urgent need to bring these systems into the 21st century to strengthen our cybersecurity infrastructure, enhance customer service for the American people, and keep pace with the rapidly evolving cyber landscape.

Since 2015, the Government Accountability Office has repeatedly warned about the Federal government's overreliance on aging vulnerable legacy IT systems emphasizing that improving the management of IT acquisition and operations must be a top priority. Today, nearly 80 percent of the billions of dollars the Federal government spends annually on IT is dedicated to operating and maintaining outdated systems, many of which are increasingly susceptible to cybersecurity threats.

For the past two decades, Congress and administrations of both parties have worked together to modernize Federal IT infrastructure. Earlier this year, Chairwoman Mace and I partnered to pass the Federal Contractor Cybersecurity Vulnerability Reduction Act of 2025 strengthening cybersecurity standards for Federal contractors by establishing vulnerability disclosure programs. This is a model of the bipartisan work we must continue.

In 2014, Congress passed the Federal IT Acquisition Reform Act, empowering Congress to better monitor agencies efforts and managing IT acquisitions. Thanks to this implementation, GAO reports as of September 2024, the Federal government has achieved $31.4 billion in cost savings. This progress reflects the impact of sustained bipartisan oversight and the creation of innovative funding mechanisms to help agencies replace aging infrastructure.

While there is much to celebrate, Congress must remain vigilant. IT modernization is not merely about upgrading systems. It is about ensuring they are secure, resilient, and responsibly managed. Recent reports have raised concerns about the Department of Government Efficiency, DOGE, efforts that may undermine the integrity of Federal IT modernization, particularly regarding the protection of sensitive data and the layoffs of critical IT and cybersecurity experts.

My Democratic colleagues and I have sent multiple letters to the Administration requesting more information about how sensitive civilian data is being safeguarded during this transition. This work requires expertise. I am concerned that funding cuts and layoffs at agencies like CISA, NIST, and DHS, the very institutions tasked with securing our government's operating system, are stunting the hard-earned progress we have made.

Cyber threats are real, constant, and evolving. We must remain ready, resilient, and nimble in the face of potential breaches by adversaries. IT modernization is a bipartisan issue. I look forward to continuing our work together on this Committee, cutting through the noise created by the reckless cuts at DOGE and focusing on the real task at hand. I am confident we can find common ground and

continue to strengthen our digital infrastructure to better serve and protect the American people.

And with that, I thank you and yield back.

Ms. MACE. Thank you. I am now pleased to introduce our witnesses for today's hearing. Our first witness today is Ms. Maria Roat, a former U.S. Deputy Federal Chief Information Officer. Our second witness is Ms. Margie Graves, also a former Deputy Federal Chief Information Officer.

Our third witness is Ms. Suzette Kent, former U.S. Federal Chief Information Officer, and our fourth witness today is Ms. Erie Meyer, a former Chief Technologist of the Consumer Protection Bureau and the Federal Trade Commission. So, we welcome everyone, and we are pleased to have you with us this afternoon.

Pursuant to Committee Rule 9G, the witnesses will please stand and raise your right hands. Do you solemnly swear or affirm the testimony you are about to give is the truth, the whole truth, and nothing but the truth so help you God? Let the record show that the witnesses all answered in the affirmative. You may sit down.

We appreciate all of you being here today and look forward to your testimony. Let me remind the witnesses we have read your written statements and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes. As a reminder, please press the button on the microphone in front of you so that when it is on and the members can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes on, your 5 minutes has expired and we will ask that you please politely wrap it up.

So, I will now recognize Ms. Roat to please begin your opening statement for 5 minutes.

STATEMENT OF MARIA ROAT
FORMER U.S. DEPUTY FEDERAL CHIEF INFORMATIONOFFICER

Ms. ROAT. Thank you. So, Chairwoman Mace, Ranking Member Brown, and honorable Committee Members, thank you for the opportunity to speak with you today. Again, my name is Maria Roat. I am the former U.S. Deputy Federal Chief Information Officer, and a retired U.S. Navy Information Systems Technician Master Chief. I spent over 40 years in the military and public sectors and a few years in the private sector, building innovative leading-edge technology solutions for many large and global Federal military entities.

I am honored to have this conversation today with you and with Ms. Kent and Ms. Graves. I work very closely with Ms. Graves at DHS and OMB, and, of course, with Ms. Kent throughout her tenure as the Federal CIO. Together we have a unique perspective of the Federal enterprise, its missions, and its technologies. We understand the interconnectedness and complexities of the Federal enterprise and the reliance of agencies on each other for information to provide services to the American public. We shaped executive orders and policies that strengthened Federal IT resilience. We

ensured agencies could continue operating efficiently despite unprecedented challenges like the pandemic and the Federal shutdown. We lived it.

I long-viewed the Federal government as an enterprise, and I think in terms of possibilities. Why not? Why do we do this that way? Who said we could not do that? Let us try it. I am by nature a risk taker, a prudent risk taker. I like to understand the what if we did X, or what if we did Y: the "so what." Asking these questions to get to a big vision always leads to creative thinking, innovative solutions, and challenging status quo to drive policy or operational changes. Again, I have done that.

With that view and my understanding of the interconnectedness of the Federal enterprise, I believe we are at another inflection point where there is even more opportunity to take the next step in IT modernization by examining the Federal government through an enterprise portfolio lens. Agencies have long worked together and shared information to accomplish their respective missions.

Many of the TMF projects reflected this interconnectedness. These modernization projects were successful because all the elements were in place. Mission alignment, agency leadership buy-in, clear understanding of the problem to be solved, contracts, multiyear funding, and the right workforce to name a few.

These projects often challenge the status quo, yet too often, one or more key elements are missing. Portfolio governance can mitigate the risks through the right oversight, the right resources, at the right time, and with the right leadership. With a Federal wide enterprise approach and asking why not and imagining possibilities, we can lead IT modernization initiatives that support effective business changes and improvements.

As we look forward, it is essential to recognize the transformative potential of newer advanced technologies and artificial intelligence to identify, accelerate, and streamline business and technology modernization projects and programs. Leveraging shared services and resources, aligning funding to portfolios, removing barriers, back to "why not," and accepting prudent risk can simplify access to government services and improve response times and enhance quality and delivery. Achieving outcomes in Federal IT modernization initiatives requires removing the barriers for information sharing and interoperability while still maintaining security and privacy. It can be done.

You will hear more from Ms. Graves and Ms. Kent on how our learnings informed enterprise solutions, like shared services, and laid the groundwork for future modernization initiatives to help Federal agencies adapt to new challenges, reinforcing the importance of cross-government modernization, cybersecurity, collaboration, and, ultimately, better citizen services.

Thank you for the opportunity to share my insights and experiences. Let us ask "what if" and "why not."

Ms. MACE. Thank you.

I'll now recognize Ms. Graves to begin your opening statement.

STATEMENT OF MARGARET "MARGIE" GRAVES
FORMER U.S. DEPUTY FEDERAL CHIEF INFORMATION OFFICER
FELLOW, NATIONAL ACADEMY OF PUBLIC ADMINISTRATION

Ms. GRAVES. Chairwoman Mace, Ranking Member Brown, and distinguished Members of the Subcommittee, thank you for the opportunity to speak with you today. I am Margie Graves, former Deputy CIO for the Federal government and former Deputy CIO for DHS, and I have spent 30 years of my career delivering technology services in the Federal government and private sector.

In my observation, the Federal government has long struggled to address the technical debt that exists within the legacy system portfolio. There is bipartisan agreement that transforming technology systems and infusing current technology into government platforms is key to mission success, yet there are several barriers to transformation that exist. Among those are a lack of committed and reliable funding sources, gaps in technology talent, and complicated and lengthy procurement processes. These barriers have hampered the ability to leverage rapidly evolving technologies in the commercial marketplace and are some of the blockers that the original Management Act was intended to address.

The vision for the MGT Act was to create a multi-year funding mechanism in the form of a government wide technology modernization fund that would be available for transformation projects whose business cases met specific criteria and provided significant value to the government in terms of enhanced cybersecurity, improved customer experience, citizen service delivery, and efficiency of operations. The selection criteria was modeled after venture capital firm operations. Key requirements that they considered include the mission impact, the solid acquisition strategy, the availability of technical talent, the selection of technologies that would be fit for purpose for this specific project, and a plan with milestones showing delivery and financial return on investment.

But even when these baseline selection criteria are met, additional preference is given to projects that address common government-wide issues where multiple departments and agencies can benefit from a proof-of-concept approach. Preference is also given to projects that integrate mission processes across agencies that share a common mission.

Finally, the adoption of shared services in the commercial marketplace is encouraged. I will illustrate these concepts with a few success stories. The Department of Housing and Urban Development executed a project that refactored legacy code of five critical business systems and moved these systems to a cloud environment. HUD subsequently provided a playbook and lessons learned to assist other agencies in taking the same path.

DHS's HSIN is an information sharing platform that played a pivotal role during COVID–19 supporting vaccine distribution and operations through the coordination of hundreds of organizations. The increased usage of this system during that time caused mission degradation. With TMF funds, the system was modernized into a cloud environment where it could scale to meet demand surge.

Customs and border protection is utilizing TMF funds to modernize systems that support better management of border security and enhance collection of trade revenue. Both of these CBP missions are executed with mission partners from other agencies, such as the Department of Treasury, Department of State, and Department of Justice. These projects demonstrate the importance of what Ms. Roat said. Taking a horizontal portfolio view of end-to-end mission operations and the systems that support them.

The Department of Energy consolidated and migrated 64 separate email systems to a unified cloud service, reducing costs and enhancing the ability to communicate with all employees. This is a clear example of adoption of commercial shared services. And as a companion piece to aid agencies in achieving shared service adoption, OMB issued memo M1916 on shared services and then worked with GSA to charter Quality Service Management Offices, or QSMOs, in the areas of cybersecurity, finance, grants, and human resources.

The QSMOs are charged with developing standards, best practices, and commercial marketplaces in these areas. In one instance, the grants QSMO has increased the adoption of shared services from 19 percent to 48 percent within the Federal grants awarding agencies.

In conclusion, the Management Act and the TMF have demonstrated success in this first cycle, and version 2.0 will continue to move the needle. I will borrow a statement generally included in most GAO reports. Much has been accomplished, and much more is needed. The technologies available to us today are even more game-changing. Artificial intelligence can now be used to refactor or create code at lightning speed. It can be used to find anomalies in cyber activity and identify anomalous activities in our benefit systems to guard against fraud and improper payments. The opportunity is there, progress is real, and TMF is one tool that will address barriers and help us move forward. Thank you for this opportunity.

Ms. MACE. Thank you.

I will now recognize Ms. Kent for your opening statement.

STATEMENT OF SUZETTE KENT
FORMER U.S. FEDERAL CHIEF INFORMATION OFFICER

Ms. KENT. Chairwoman Mace, Ranking Member Brown, and Ms. Ansari, thank you for the opportunity to speak with you today. I am Suzette Kent. I served as Federal Chief Information Officer during President Trump's first term, and I have spent over 30 years in the private sector building and operating technology solutions for many of the world's largest companies.

Ms. Roat covered the importance of approaching government modernization as an enterprise and the connected nature of technology and data across agency missions. She has shared some successes, but highlighted barriers. Ms. Graves spoke about the impact of the technology modernization fund. She also summarized steps that we took in previous administrations to drive common technology for common services and she shared progress, yet there is still so much to do.

I would like to build on their comments and state why I believe that we are finally at a juncture where it is possible to take down this legacy technology hurdle. In the office of the Federal Chief Information Officer, we often use the language of OMB management memos and the expectations of law to define our technology goals, but I am going to use plain language today to point out that much of the needed policy and law that defines what the technology goals should be are already in place.

Things like eliminating inefficiency, fraud, and waste; achieving security and resiliency in all mission spaces; common government tools for common processes; prioritizing the use of scalable security hardened commercial solutions; and use of data in advanced technologies to eliminate manual activities; and finally, deployment of digital solutions for critical government service.

So, if our goals are defined, how do we get there? As you consider this question, there are now two things that are modernization game changers. The first thing, it is thrilling to think that modernization is finally a top priority. The actions being taken through executive orders, streamlining of acquisition at GSA, proposed policy changes, and updated laws like the Modernizing Government Technology Reform Act loudly signal that Congress and this Administration understand that achieving efficiency and delivering effective mission outcomes requires modern technical capability and bipartisan collaboration.

The second thing is the extraordinary advancement of the tools to drive modernization efforts. I work directly with many of the companies who build code assistance tools, deploy automation at scale, and leverage large language models to unlock the power of data. Over the past few years, these companies have unleashed new accelerators that redefine the expectation of time, of cost, and the risks of modernization. This is not hype or promise of what is to come. These results are real, and they are repeatable.

So, what does that look like in government? I am going to leverage the examples that Ms. Roat and Ms. Graves shared. That HUD project with the tools available 6 years ago, that process took multiple years and cost over $5 million. That effort did define a path forward, but today we can travel that path in months versus years with a tenth of the price tag because of the advancement of code assistance tools.

The CBP project reference, they retired a 30-year-old main frame that tracked imported and exported goods. They recently celebrated the retirement of that outdated system, but that took many years of work. Their efforts helped pinpoint the types of roadblocks that must be eliminated to speed up future efforts. And both Ms. Roat and Ms. Graves reference an experience taken on by four agencies to share data. That initiative was a catalyst to identifying the types of efficiencies possible with cross agency data sharing. Today, modernization success can be unlocked for every agency. With continued leadership priority to remove barriers and leveraging the commercially products and tools, it makes modernization less complex, less costly, and, importantly, less risky.

There is one additional piece of the modernization puzzle that should also be considered: to sustain a leaner highly efficient operating environment, agencies require people who understand the

new technology. Investments in upskilling the Federal workforce and establishing expectations for continuous skills advancement are required as the government aspires to get maximum value from the technology it implements. This is the last piece of the puzzle to sustaining efficient operations.

In closing, the keys to unlocking government efficiency through technology are actually in reach. By making modernization a visible priority, holding agency leaders accountable for making progress, and embracing commercial modernization tools, Congress and the Administration can open the door to a new reality for achieving government efficiency. Thank you.

Ms. MACE. Thank you.

I would now like to recognize Ms. Meyer for your opening statement.

STATEMENT OF ERIE MEYER
FORMER CHIEF TECHNOLOGIST
CONSUMER FINANCIAL PROTECTION BUREAU AND
FEDERAL TRADE COMMISSION

Ms. MEYER. Thank you. Chairwoman Mace, Ranking Member Brown, and Members of the Subcommittee, thank you for the opportunity to testify today. My name is Erie Meyer, and I am the Founder of the United States Digital Service, a former Chief Technologist at both the Consumer Financial Protection Bureau and the Federal Trade Commission, and someone who has spent my career working to make technology serve the American people more fairly and securely. I have helped veterans and students apply for assistance online. I have led efforts to root out fraud and abuse in the financial and tech sector. I have brought technologists, hundreds of them, into government to solve problems that matter, like streamlining seniors' access to benefits and protecting children's data.

I believe deeply in the promise of public sector technology. Done right, it can save money, reduce fraud, and make government work better for everyone. I have seen it happen.

But what is happening right now under DOGE is not modernization. It is chaos, and it is chaos with a human cost. When DOGE arrived at my agency, they did not modernize anything. Instead, they broke the consumer complaint system that the CFPB runs per congressional mandate. As a result, at least 75 families facing imminent foreclosure of their homes were left in limbo. Service members could no longer submit banking statements to report being illegally overcharged in interest. More than 16,000 consumer complaints were stuck in the system with no path forward. Even congressional offices, your offices, could no longer refer constituents to the CFPB for help.

The damage is harming industry too. For example, DOGE staff demanded God-tier access to confidential investigatory data about the consumer finance market right as Elon Musk has been preparing to launch the X payments financial services product. In court this week, a Federal worker submitted testimony that DOGE had planned actions that would break a rate spread calculator critical to processing mortgage loans. She explained that if that tool

broke, it would halt or severely disrupt mortgage lending across the country.

AI experts, security professionals, people who were working to protect kids online, stop fraud, and keep our system safe have been fired or simply driven out. And while this is happening, DOGE is centralizing access to some of the most sensitive data the government holds: social Security records, disability claims, even data tied to national security without a clear plan or proper oversight.

Further, I question the basic vetting of the AI tools they are using to analyze this data. Let me be clear. This is not modernization. It is a heist. The cheapest, fastest, and most effective way to modernize IT in the Federal government is to fund programs like the technology modernization fund, and to get technical people into government, and then to empower those people. They have taken an oath to serve, and they want to do good work. The most expensive, slowest, and least effective way is to lose all of your technical talent.

When our parents log into their Social Security accounts, they want to know that the people who build and maintain that system are qualified professionals who take security seriously. There is even rumors now that Federal workers will be replaced by chat bots. At CFPB, I led research on chat bot performance in the banking sector. We found that some of the worst outcomes happened when people were trying to report fraud. Seniors got stuck in doom loops and wrote in to us to say things like, I cannot get a human on the phone. It is not modernization. It is abandonment. DOGE is burning down the house and calling it a renovation. This path is making government less efficient, less secure, and less capable of protecting the people it is supposed to serve.

I urge this Committee to look past the slogans and ask: Who benefits from these changes? Is the chaotic hatchet approach going to serve the public or will it serve private interests? I am here today because I still believe in what is possible. I have seen dedicated public servants like the women next to me use technology to save money and change lives. When IT modernization is done right, it makes the government work better for everyone. Thank you and I look forward to your questions.

Ms. MACE. Thank you so much.

I will now recognize myself for 5 minutes. My questions are kind of, I think, going to generally be to everyone on the panel this afternoon. My first question is your opinion, what are some of the biggest barriers that obstruct change? Do you think it is procurement requirements, hiring processes, budget limitations, which we know that is not—that is, no. Do not even bring that up. Or bureaucrats? In your opinion, what is the biggest barrier? We will start with you, Ms. Roat.

Ms. ROAT. Thank you, Chairwoman. So, when you really look at the barriers to change, it takes many things to happen, right? We have talked about the funding, right? Multi-year funding. But it also is, you know, the leadership, the project management. It is all of those things coming together.

Ms. MACE. I think you mean bureaucrats, right?

Ms. ROAT. What is that?

Ms. MACE. Bureaucrats?

Ms. ROAT. Yes, ma'am. When you are trying to get something done and having that vision, and here is what we are going to do, and even that partnership with the business office, because you are not modernizing technology for technology's sake. There is also going to be a services outcome to that, and the business has to be a partner in that.

I have worked on projects even since I retired supporting projects where the business would not come to the table. Well, you know, doing any technology modernization without having the business to help improve the services to automate——

Ms. MACE. I am going to let Ms. Graves; the next one. I have a couple questions I want to ask.

Ms. Graves, what is the biggest barrier?

Ms. GRAVES. I would say that the biggest barrier is probably the senior support and continuous senior support. A lot of times, there are competing priorities within the agency for funding and IT can sometimes take a back burner position because it is working. It is not working well. It needs to be modernized. But meanwhile, we have got something else over here that we need.

Ms. MACE. That is broken.

Ms. Kent?

Ms. KENT. I would echo the support from the top. Every one of the successful examples that were shared had an agency Secretary that leaned in and said we want to get this done and ensure there was funding, that we moved fast through procurement, and that the outcome was measured. I think the legislation that this Committee has proposed actually has some language to actually measure that results are being delivered and hold individuals accountable, and I think that actually moves the needle.

Ms. MACE. Ms. Meyer.

Ms. MEYER. I would agree with my two co-panelists, specifically that executive sponsorship with the right goals in place. Things should simply just work for veterans. They just should. And there should be cover and support for making that come true.

Ms. MACE. And it is difficult to even navigate the veterans' website. I mean, it is crazy how difficult it is. And then, Ms. Meyer, we will start with you and work backward. What is the single most important thing the Trump Administration should do to modernize Federal IT? What is the one thing? If you do only one thing right now, today, and wave a magic wand, what is that one thing that would make a difference?

Ms. MEYER. I am concerned that the reckless and dangerous approach is going to set us back.

Ms. MACE. What is the one thing you could do? I get what you would disagree with, and your statement was very clear on that, but what is the one thing you could do right now to wave a magic wand to have this Administration modernize our IT quickly? What is the one thing?

Ms. MEYER. I would re-hire 18F, which is full of open-source software, engineers, designers, and the people I called when I was canceling contracts that were rotten to the core. They were the people that we could bring in quickly to keep things moving.

Ms. MACE. OK.

Ms. Kent?

Ms. KENT. I would take that GAO list that is appalling and make it first priority and say plan it, fund it, and measure that it gets done.

Ms. MACE. OK.

Ms. Graves.

Ms. GRAVES. I would take a portfolio view of that GAO list, and I would look for common solutions that could uplift multiple agencies if they were implemented.

Ms. ROAT. And I will add on to Ms. Graves and say that portfolio approach when you look at the cross-cutting funding for across the Federal government, you can achieve some efficiencies and address the gaps.

Ms. MACE. What do you think about our procurement process? Is there, like, contracts? I am currently getting information about a particular contract where this big IT company has come in and they have, like, three, four, five times the number of contractors managing a very small group of technology workers within the U.S. Federal government, and on top of that, about half the employees. We are talking hundreds of people here for hundreds of millions of dollars in this contract, hundreds of people just sitting on the back bench doing nothing. So, like, is this a thing that goes on in the government, this kind of procurement or contract?

Ms. ROAT. So, in my personal experience, I did not have a lot of patience for that. I looked for——

Ms. MACE. But it goes on, right?

Ms. ROAT. I looked for opportunities to say, "What are you doing," "Why you walking around with that coffee cup?"

Ms. MACE. Ms. Graves, do you see this kind of thing?

Ms. GRAVES. Yes. The justification of every person and what their contribution is to the project is something that the Federal employees need to make sure happens.

Ms. MACE. Ms. Kent? Running out of time. Real quick.

Ms. KENT. I think the efforts that are being taken for agencies to work more closely with those who are providing the technology lets us eliminate to maybe people who are not delivering value, and then I do think, my last point, where we have to address upskilling the Federal workforce to make sure that the technology that is being implemented, they know how to get the value out of it.

Ms. MACE. Ms. Meyer.

Ms. MEYER. I think funding TMF is the only way to fight back on things like that, because it incentivizes the right practices in a flexible way.

Ms. MACE. All right. I will now recognize the Ranking Member for 5:33 seconds to make it even.

Ms. BROWN. Thank you, Madam Chair.

The nonpartisan Government Accountability Office has been warning for decades that we need to improve management of IT acquisition and operations. One of GAO's most urgent recommendations is ensuring that Federal agencies have a skilled and capable IT workforce. This is a nonpartisan issue. It should not be a partisan issue. Democrats and Republicans agree upgrading our crumbling tech infrastructure requires tech-savvy professionals.

And actually, the Chairwoman and I have both worked on separate bills that aims to remove barriers and the red tape in the pipe-

line for IT talent. Yet this year, we have seen more than 200,000—200,000—probationary employees cut across various Federal agencies in the name of government efficiency. Many of them are the exact IT and cybersecurity experts we desperately need to modernize government systems and to respond to cyber threats.

Modernizing government systems is about more than just efficiency. It directly improves the lives of everyday Americans. For example, under the Biden Administration, the IRS launched a free direct file tax website providing another option for people filing their taxes. However, the current Administration is moving to dismantle this service. Across the Federal government, similar consumer facing technology projects are being gutted, threatened to delay updates that would benefit Americans nationwide.

So, first I want to thank you, Ms. Meyer, for your courage in speaking out about what's really happening at the Consumer Financial Protection Bureau under the banner of modernization. It is clear from your testimony that it is not just a case of mismanagement. It is a systematic gutting of protections for consumers, veterans, and seniors. Can you tell us more about your work and why every American should be alarmed by what happened at the CFPB?

Ms. MEYER. Yes, and thank you for the question. Part of my job was to make sure that regulators were ready for big tech who was lurching into consumer finance. We did not think it should be the case that if you have a brick-and-mortar financial company or bank, you should be playing by a different set of rules than big tech when they decide to offer one of these services.

One of the first things that DOGE did after they arrived at my agency was to fire every single technologist who we brought in. They had come in from technology firms, some were professors of computer science. We have a veteran who is an expert in robotics. They were all fired in one fell swoop, and it was really concerning that the people who were supposed to be watching and protecting to make sure that seniors—all these communities that are typically targeted—were not being unfairly exploited on these big tech platforms, while brick-and-mortar financial companies had to follow a different set of rules.

Ms. BROWN. Thank you. And so let me ask you this. Can you tell us why having qualified modern IT workforce is not just important, but essential to security, efficiency, and effectiveness of Federal systems?

Ms. MEYER. Without the right people on board who have taken the oath of office, have completed their ethics vetting, and have no other masters, you have serious questions about the conduct in place. For example, the work of 18F and other open-source projects in government have saved millions and millions of dollars in front of my eyes, because we can reuse those public artifacts. We can reuse the things that they have started in a way that is just not possible on some contracting options.

The other big benefit is they can help with hiring. My team hired 25 technical experts, and we were able to collaborate with technical people from across the government to streamline hiring to get technical people in faster, pooled hiring, and I think most of those peo-

ple that we worked with are now gone. I do not know how you would do that now.

Ms. BROWN. Thank you. One of the promises of technology modernization is to make government services more accessible to all Americans, especially underserved communities. Can you speak to some of the consumer facing aspects of government technology modernization that we have come to rely on and explain the impact that Federal staffing cuts have had on these programs?

Ms. MEYER. I will use one specific example. There is a team of technical experts who worked at the Social Security Administration, the Office of Technology Transformation. Their entire job was to get rid of wet signatures, to let people file things online or over the phone. They were all fired at once without any notice, and what that means is—the reason I found this out is because a friend said my mom is having a really hard time getting through to the Social Security office, do you know anyone? I reached out to friends I knew that had worked there, and they said you know what, she is probably going to go have to stand in line, because the people who would fix this kind of thing are not there anymore. By the way, I just got fired. It was devastating.

Ms. BROWN. Thank you again. As I stated before, this is not a partisan issue. We must work together to ensure that the government's technology is modernized to strengthen cybersecurity and to keep Americans' data secure and improve customer service, so thank you, Madam Chair, for the extra couple seconds, and with that I yield back.

Ms. MACE. Thank you. And I will now recognize Representative McGuire for 5 minutes.

Mr. MCGUIRE. Thank you, Madam Chair, and thank you to our witnesses for being here today. It is no secret that our government is not as efficient as it could be or should be. A large part of that inefficiency stems from outdated technology. Outdated systems not only stifle efficiency but also leave us vulnerable to security and operational risk. So, a question for all the witnesses, yes or no, very simple, modernizing legacy IT systems in the Federal government would improve efficiency, yes or no?

Ms. ROAT. Yes.

Ms. GRAVES. Yes.

Ms. KENT. Yes.

Ms. MEYER. Yes.

Mr. MCGUIRE. All right. We are moving in the right direction. All right. President Trump implemented DOGE to help modernize legacy IT systems in the Federal government. DOGE has been working hard to root out waste, fraud, and abuse. Within the Federal government has taken steps to modernize outdated systems. In February, DOGE highlighted the OPM Retirement Operation Center where around 10,000 Federal employees' retirements are processed by hand using paper every month. This facility is located about 230 feet underground and paper files are transported to the mine daily in trucks where workers manually review, calculate, and approve benefits before sending the paperwork back to D.C. I mean, it is 2025. So, our question for all the witnesses, again, yes or no, do you believe this is the most efficient way to process Federal retirement paperwork in 2025?

Ms. ROAT. No.
Ms. GRAVES. No.
Ms. KENT. No.
Ms. MEYER. No.
Mr. MCGUIRE. You guys are getting a great grade on your report card. All right. The mine filled with paperwork is indeed not the most efficient practice. A 2019 GAO report found that OPM failed to meet its goal of processing most retirement applications within 60 days, between 2014 and 2017, largely due to reliance on paper-based applications and manual processing as well as insufficient staffing. So, question for Mrs. Graves and Mrs. Roat. Mrs. Graves and Mrs. Roat, how might agencies work with DOGE to improve government-wide shared services? We will start with Ms. Graves.
Ms. GRAVES. I think that the most important thing that we need to do is look at that portfolio of systems that we have in the Federal government and identify common solutions. And once we identify those common solutions, we can create shared services to support those solutions over time and let the agencies avail themselves of these common solutions.
Ms. ROAT. And I would add on, it is not just the shared services. When you look across the Federal portfolio, there are often times agencies that work together, four agencies, five agencies on a particular mission, so looking at that the portfolio, there are opportunities even beyond shared services to really improve how the agencies work together and provide those services.
Mr. MCGUIRE. Thank you. We do not have a lot of time, but a question for all the witnesses. And we will start with Ms. Meyer. Where a large-scale Federal IT modernization efforts have failed, what, in your opinion, are the primary reasons for those failures?
Ms. MEYER. I think people need to spend more time listening to veterans and seniors about what their experience is like. Many agencies I have worked with had never watched someone try to use their system before, and in some cases, a backlog existed because the person kept hitting submit over and over again, not because the whole system was broken. So, I think sitting down and listening to our seniors and our veterans directly as they try to use services would make a huge difference.
Mr. MCGUIRE. Thank you.
Ms. Kent?
Ms. KENT. If I am using the examples of what failed, managing the scope and the initiative to what they started with and holding the agency accountable for delivering on the project as it was intended is one of the areas where we have seen things deviate and change as they worked through the project, and not rechecking that initiative against the intended outcomes for which the project was started.
Mr. MCGUIRE. Mrs. Graves.
Ms. GRAVES. I think the thing that I would emphasize is the fact that many of these portfolio programs are dependent upon different funding streams from different agencies, and what we have to make sure happens is that the coalition holds together as the program is executed so that each funding stream that is part of that total equation is actually there and ready for use when the program reaches the need for it.

Mr. MCGUIRE. Thank you.

Ms. Roat.

Ms. ROAT. I would add on that I have seen where leadership priorities, when leadership turns over, when there are changes, whether it is the CIO level or the front office, and the support is not there for the project to sustain it year over year, whether there is funding or not, but making that a priority, that is where I have seen some of these large scale programs fall apart.

Mr. MCGUIRE. Thank God we got President Trump and Elon Musk and DOGE taking it seriously. If a government was a business, it would be out of business.

With that, I yield back. Thank you.

Ms. MACE. Thank you. I now recognize Representative Ansari for 5 minutes.

Ms. ANSARI. Thank you, Chairwoman.

Elon Musk claims that he is tackling government inefficiency and improving the technology that the Federal government relies on, but there has been no evidence that Elon Musk and DOGE—there has been no evidence that they are modernizing or improving anything. In fact, they are weaponizing access to Americans most sensitive data under the guise of innovation, and in the process, turning the Federal IT systems into a playground for reckless amateurs.

In just a few months, DOGE has bulldozed basic data protections, handed over sensitive information to unvetted AI companies, and exposed national security systems to potential foreign threats. Now they are wreaking havoc at the Social Security Administration, a lifeline for millions of Americans, and according to whistleblowers, DOGE is actively sabotaging Social Security operations by cutting staff, disrupting IT systems, and launching an ill-prepared overhaul that is nothing short of a data grab. They are reportedly illegally throwing a massive data base by pulling data from across the Federal government with zero oversight or legal authority. In my view, this is a systematic attack on Americans privacy.

Ms. Meyer, DOGE claims it can rip out and replace the Social Security Administration's decade-old IT system, which is critical for processing Social Security payments in a matter of weeks. SSA experts say it will take at least 5 years.

Ms. Meyer, in your expert opinion, is it even remotely possible to replace a mission-critical Federal IT system in weeks without a plan, without preparation, and without experienced professionals?

Ms. MEYER. No.

Ms. ANSARI. And Ms. Meyer, why is that?

Ms. MEYER. It is because the data we are talking about is not some abstract concept. It is the concrete details of my mom's life and finances. It is her home address. It is how she hopes to survive during her retirement. Sloppy and chaotic destruction of systems and exfiltration of data introduces risks that are hard to conceive of.

Much of this information, it is immutable data. She will never have some of these facts be different about her. And when you consider that happening at scale to an audience that is often already targeted for fraud and scams, we are introducing an extraordinary

amount of risk to some of the most vulnerable people in the country.

Modernizing systems should be done with people who are committed to security and modernizing using the most important protections that we have in place to protect our seniors' data.

Ms. ANSARI. And DOGE is also reportedly handing over Federal job functions to IT solutions that use AI. How does the use of AI in place of Federal workers hurt not just the workers themselves, but the American people at large?

Ms. MEYER. I think when people reach out to a government office for help, they want to get that help. I think that when things break, or you get stuck in a doom loop or you get an answer that does not make any sense or something is not answering the question you asked it, it is incredibly frustrating. I think that research has shown that many of the modern AI systems can continue to contain hallucinations.

I believe in technology. I believe in public sector technology, people like Grace Hopper and Katherine Johnson who worked for the government when they led the future of science and technology. I think slapping together unproven tools on the services that veterans and seniors are counting on is totally insane and reckless.

Ms. ANSARI. Committee Democrats have been told that DOGE is combining sensitive legally protected information from SSA, the IRS, HHS, and other agencies into a singular unauthorized mega data base. DOGE staff are walking around with backpacks full of laptops loaded with access to different Federal systems and American sensitive data, stitching together data that, by law, must remain separate. This is not just dangerous. It is blatantly illegal. The Privacy Act was designed to stop exactly this kind of overreach. DOGE is bulldozing those legal safeguards, putting American's Social Security data, health records, and tax information at risk all without oversight, consent, or justification. So, Ms. Meyer, does DOGE seem to be complying with the Privacy Act in its creation of this cross-agency master data base?

Ms. MEYER. No ma'am.

Ms. ANSARI. And when you were the chief technologist at CFPB, would you have ever been allowed to access and merge sensitive data from across the Federal government into one centralized system using backpacks full of laptops collected from different agencies?

Ms. MEYER. Never. It is unheard of.

Ms. ANSARI. And, Ms. Meyer, why would you not have been allowed to?

Ms. MEYER. Part of the way that we keep data secure is not by giving access to people who do not need it for their job function. I worked with every single part of the Bureau as an executive of the agency. That does not mean that I needed every piece of data, every piece of personal information from every single division in order to work. It was important for security that we were each constrained to not have more than we needed. It makes you a target for attacks, it introduces other risks to people, and it was unfathomable even for modernization that you would start and end with slapping everything together in a janky data base.

Ms. ANSARI. Thank you. I yield back.

Ms. MACE. Thank you. I will now recognize Representative Burlison for 5 minutes.

Mr. BURLISON. Thank you, Madam Chair.

Having worked in the private sector and IT for 20-plus years, I have seen it all. I have seen a lot. I have seen a lot of waste. I can only imagine how wasteful the Federal government is when it comes to software contracting.

Mrs. Kent, the Department of Housing and Urban Development moved from a legacy common business-oriented language application to a more modern code base with tools that are available 6 years ago. That process took multiple years and cost over $5 million. You stated that that effort, if it were to be done today, would take months versus years with a tenth of the price tag. Can you elaborate on that?

Ms. KENT. Certainly. When we started that project, and it was a project under the technology modernization fund, the agency was using the code assistance, or code translation tools, that were available at the time. And what they were doing was actually testing the accuracy of the ability to go from 11 million lines of code, which was the set of applications, to more modern, which, by the way, they got it to 3 million. But the tools at that point in time only had about a 75, 80 percent accuracy, which meant somebody actually had to go in and translate, you know, hands on keyboard, do the rest of that work.

The tools—and then my written testimony had some examples. The tools that are available now, the code assistance tools, are operating at a 97 and 98 percent accuracy in many cases. They are also significantly less expensive. So, as time has passed, those tools have become less expensive, so I use that as an example. The work at the time was important, it was groundbreaking, and it was a step forward for HUD. But as we think about other agencies who have not taken those steps forward now, the complexity, the risk, the time, and what it will cost us will be significantly less.

Mr. BURLISON. Working in the health care system in IT and IT procurement, we would often have vendors that would go to the different agencies, and we would have situations on occasion that would pop up where one department was not talking to another department, and the vendors love this, because they get to sell an organization both products, right? Two different completely different products from different companies for the same solution all being very wasteful. Is that something that occurs regularly within the Federal government?

Ms. KENT. Unfortunately, it does. I think that is why some of the efforts for visibility, clarity, and the discussions with many of the vendors looking at, as Ms. Roat pointed out, the government as an enterprise as a whole. There were efforts that I took on as Federal CIO to actually bring that visibility across government and clarity to what agencies were buying, and more importantly, what they are using, and that is an effort that needs to continue.

And I think we have seen Members of Congress actually put forth some legislation to help and to make that a—something that agencies are held accountable for, but also in changing the dialog with many of the vendors that serve the government, making sure that we are looking at taking that enterprise view.

Mr. BURLISON. Yes. One of the axioms when you are in that world is that the more that the clients wants to customize and not change their processes, the more expensive and the longer it is going to take. Do you have—I am thinking of the VA, the implementation of the electronic medical record of the VA. From what I am told, it was required that they have a completely new site, customized site for every location in the VA. Do you have any insights on that or—Mrs. Roat, I do not know if you have any insights. Or to—my question is, who is minding the farm when it comes to—or kind of wrangling these agencies in? Because it is just a common desire to want to force the code to adopt to your processes as opposed to adopt the best practices and the processes of the industry. And so, do you get what I am asking?

Ms. ROAT. Yes. So, I get exactly what you are saying, because part of the challenge is, when—you want to standardize, say, on a case management system, right? That is not just about the technology that you are modernizing, moving to some case management. The business has to be a partner and has to be at the table. And that is where, when you talked about the processes were not modernized, this is where, when you are trying to automate, you are trying to—you know, technology is the enabler, but unless the business has a seat at the table for one, and they want to be there, they have to be a part of the solution. That is the only way that you are going to improve and get better outcomes on the end.

And I have done this in practice, exactly that, where I have had challenges with the business on being that good partner, and I have also had good business partners where we were able to move very quickly, move to, say, a case management system where you were automated and where you had better results for the services you were providing.

Mr. BURLISON. But you see customization rampant throughout the Federal government, Ms. Kent? I am seeing a head nod.

Ms. KENT. Yes, especially as we were talking about modernization on those older systems, absolutely.

Mr. BURLISON. And that is expensive, outrageously expensive. Thank you.

I yield back. My time is long expired.

Ms. MACE. OK. We are stalling, so we want to wait for a minute or two. I am going to ask—is it OK with you? I am going to ask a few questions while we wait for your colleague to come and do his 5 minutes. He should be here any minute now.

Again, my question is for the panel. I will start, Ms. Kent, with you. How important is modernizing our technology, government technology, due to cybersecurity threats? Like, what kind of vulnerabilities by not modernizing does this put us at from a national security standpoint?

Ms. KENT. Thank you for that question. I think both you and the Ranking Member made points about cybersecurity, and when you look at what is spent in the Federal government, much of those funds are around securing these outdated systems. So, whether we look at cyber or we look at the quality of the services that are delivered.

Also, many of these older systems, when we change something, it takes a long time to do it, and we do that with less accuracy with many of these outdated systems.

You also heard some things of unintended consequences. We do not understand clearly sometimes where they are connected. There was a question from Mr. McGuire about retirement and paperwork and wet signatures. We also saw those during COVID. We saw systems break where we did not understand the connectivity. So, it costs us in security, it costs us in dollars, and it costs us in the quality of services that government can deliver.

Ms. MACE. Does anyone else want to also comment? Ms. Graves?

Ms. GRAVES. Yes. I think one of the things that we looked at when Ms. Kent and I were working together at OMB was the establishment of an inventory of your high-value assets. What are the most critical assets with the most critical data, that if that data is leaked or if that data is misused would cause significant harm. And then we put those on the master list to actually become more cyber secure and to take them into a modernization effort earlier rather than later, and make sure that we were addressing those based on priority. I think that went a long way toward helping people understand how important it is, and a lot of people who are in Federal agencies do not necessarily understand the cyber aspect of the mission system. They understand what the mission system does, but all of the wrappers that go around it are equally as important.

Ms. MACE. Ms. Roat.

Ms. ROAT. I will add on that even when you have legacy systems, there are steps you can take to mitigate and minimize those cyber threats. Like one agency specifically where they have a legacy mainframe, they did put on the front end for the log-in for the public and staff, multifactor authentication. At least that is something better than nothing when it was a log-in and password.

So, on top of what my colleague said, there are steps you can take, but it is hard, and that does not mitigate the entire threat, but at least it is a step in the right direction.

Ms. MACE. OK. Ms. Meyer, did you want to chime in on that?

Ms. MEYER. Yes, I agree with what has been said. I would also say that even when we are not talking about high-value assets, sometimes a lot of boring data when put together can be really dangerous. So, one of the things that I think is really tough is that there is no cloud-based password management system available to Feds today. Right now, Feds are emailing each other shared spreadsheets titled, password. And I will let you guess what is in there. And it is really dangerous.

Ms. MACE. Password: One, two, three, four.

Ms. MEYER. Yes, over and over again. Whereas modern systems, we can buy software. Anyone can buy software that says, Hey, this password has been compromised, Hey this is not strong enough, and to protect them. And I really hope Feds get access to those tools, too.

Ms. MACE. OK. I will ask you one more round of questions since I am dying about this while you get your remarks prepared. One more minute.

The advent of AI and what it can be used, bigger, better, faster, more safer, more secure, just comments on—I just—we have so much money the government can spend. There is just so much opportunity here to invest in high-speed tech that can help us. Why are we not using AI to make it all better, faster, more? Ms. Kent.

Ms. KENT. AI brings lots of potential, but it still requires someone who understands the mission. And all the requirements of responsible security, those things are exactly the same. And many of the AI tools will bring that efficiency, and we have significant opportunities. But that has to be coupled with mission intent, understanding of the data, and people who understand how to use that technology.

I think we are seeing successes across private sector because they started earlier and focus on improving those systems. We had that same opportunity in government to move more quickly and to operate with intent.

Ms. MACE. OK. And I am now going to recognize Representative Subramanyam for 5 minutes.

Mr. SUBRAMANYAM. Thank you, Madam Chairwoman. Great to be here, and thank you for this very important hearing. I have a lot of folks in my district who are actually IT experts who do a lot of great work for our Federal government. And so, they often took lower pay to come to the Federal government to lend their expertise. And from talking to many of them, right now their morale has never been lower. And at a time where we need to modernize our IT systems when you have the best technologists in our Federal government, or at least working with our Federal government, I am worried that we are going to have a brain drain when it comes to technology expertise.

And so, I know some of you have worked in this space in the past. And, you know, one of the groups that, you know, I really enjoyed working with during my time of the Obama Administration was 18F, and on March 1, DOGE eliminated 18F

I am just curious, Ms. Meyer, do you know about 18F, and can you tell me a little bit about some of the important work important that it does?

Ms. MEYER. Thank you for the question. 18F is a team of Federal workers under oath, most of whom left the private sector or other high-profile jobs in academia or elsewhere to come serve their country. They often took pay cuts. And the work that they do exclusively makes things cheaper, faster, better, and more reliable. I have worked with them on a number of different projects. Every single time that they touched a project, at least for me, it was millions of dollars less than it would have been.

One time there was a contractor that I was working with, and they just clearly could not do the technical work. It was just obvious that they were unable to do some basic technical tasks. And the contracting officer at the agency said, well, if you cancel this contract, we do not have enough time to startup a new procurement from scratch. Like it is just impossible. And we were able to sign an interagency agreement to get 18F in, which allowed to us to cancel the contract with a firm who was maybe great at winning contracts but not great at actually delivering and really worried about that capacity being missed.

Mr. SUBRAMANYAM. And some of the work they were doing is improving access to National Weather Service data, modernizing our tax filing system. And this was deemed noncritical, but would you consider a group like 18F critical?

Ms. MEYER. I think not only they themselves are critical, but their presence in the Federal government to help every other critical agency would was critical, too.

Mr. SUBRAMANYAM. And the U.S. Digital Service, I believe you worked there, it is now the U.S. DOGE service, I believe, and they were doing really important work as well. And I am just curious, you know, what could we do to support the work that they are doing and move that forward at this point?

Ms. MEYER. Yes, so I understand that your Subcommittee has been excellent at connecting with whistleblowers. I am contacted every day by Feds who are trying really hard to uphold their oath of office to the Constitution. And you all are a body that they really trust. Again, in the bipartisan nature, this group is really fighting to help the United States be safe and secure and work properly. So, I think continuing the work with whistleblowers.

I think it was devastating that every single designer and contracting expert at the U.S. Digital Service was fired at once. When I talk about listening to veterans or seniors to understand how something works, that was the team that would have done that. When we talk about buying technology that works rather than buying people who kind of sit around, those contracting experts are the exact people you want in the room. And I think that morale is really low.

I worked in the Administration when Trump was the President last time, and people were still able to help people. So, they were willing to work with whatever party. They do not care. They do not want to talk about politics at work. They want to talk about veterans. They want to talk about helping people.

Federal IT should be boring. It should just work. We should not have to think about our taxes. It should just happen. But I have found that people are really devastated and torn and are really struggling with how to uphold their oath of office and how to get this really important work done.

Mr. SUBRAMANYAM. And one of the things that I did in the Administration, you did as well, was try to attract and retain great technology talent within the Federal government and also forge connections with great contractors who can do great work as well. I have heard from a lot of constituents, who are technologists, who say now they would never work for the Federal government given what is going on now.

What can we do to reverse course on that? And what can we do to attract technology talent?

Mr. MEYER. I think it is critical that this body and every oversight body very carefully respond to the violations of the Federal law. I think people do not want to be asked to do illegal things at work. I think they do not want to be asked to exploit people who are just trying to pay their bills and survive. I think careful oversight of where the law has been broken, enforcing the laws that are on the books—this does not have to be creative. Whether it is the Privacy Act, any of these rules, making sure that they are upheld

and not letting people off the hook would give people confidence that they really can come back and serve and will not be asked to do inappropriate things.

Mr. SUBRAMANYAM. Thank you. I yield back.

Ms. MACE. Thank you. In closing, I want to thank our panelists once again for their testimony today.

And, without objection, all Members will have 5 legislative days within which to submit materials and to submit additional written questions for the witnesses which will be forwarded to the witnesses for their response. If there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 3:32 p.m., the Subcommittee was adjourned.]