AGENCY COMPLIANCE WITH THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA)

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

APRIL 16, 2021

Serial No. 117–14

Printed for the use of the Committee on Oversight and Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE

44–381 PDF WASHINGTON : 2021

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
RASHIDA TLAIB, Michigan
KATIE PORTER, California
CORI BUSH, Missouri
DANNY K. DAVIS, Illinois
DEBBIE WASSERMAN SCHULTZ, Florida
PETER WELCH, Vermont
HENRY C. "HANK" JOHNSON, JR., Georgia
JOHN P. SARBANES, Maryland
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
MARK DESAULNIER, California
JIMMY GOMEZ, California
AYANNA PRESSLEY, Massachusetts
MIKE QUIGLEY, Illinois

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
PETE SESSIONS, Texas
FRED KELLER, Pennsylvania
ANDY BIGGS, Arizona
ANDREW CLYDE, Georgia
NANCY MACE, South Carolina
SCOTT FRANKLIN, Florida
JAKE LATURNER, Kansas
PAT FALLON, Texas
YVETTE HERRELL, New Mexico
BYRON DONALDS, Florida

DAVID RAPALLO, *Staff Director*
WENDY GINSBERG, *Subcommittee Staff Director*
TAYLOR JONES, *Clerk*

CONTACT NUMBER: 202-225-5051

MARK MARIN, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

ELEANOR HOLMES NORTON, District of Columbia
DANNY K. DAVIS, Illinois
JOHN P. SARBANES, Maryland
BRENDA L. LAWRENCE, Michigan
STEPHEN F. LYNCH, Massachsetts
JAMIE RASKIN, Maryland
RO KHANNA, California
KATIE PORTER, California

JODY B. HICE, Georgia *Ranking Minority Member*
FRED KELLER, Pennsylvania
ANDREW CLYDE, Georgia
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
YVETTE HERRELL, New Mexico

C O N T E N T S

INDEX OF DOCUMENTS

Documents entered into the record during this hearing and Questions for the Record (QFR's) are listed below.

Documents are available at: docs.house.gov.

AGENCY COMPLIANCE WITH THE FEDERAL INFORMATION TECHNOLOGY ACQUISITION REFORM ACT (FITARA)

Friday, April 16, 2021

HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND REFORM
Washington, D.C.

The subcommittee met, pursuant to notice, at 9:03 a.m., in room 2154, Rayburn House Office Building, Hon. Gerald E. Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Davis, Porter, Hice, Keller, Biggs, and Comer (ex officio).

Mr. CONNOLLY. This subcommittee will come to order.

Some witnesses and persons and others will appear remotely via Zoom today. Since some members and witnesses are appearing in person, let me first remind everyone that pursuant to guidance from the House Attending Physician, all individuals attending this hearing in person must wear a face mask. Members who are not wearing a face mask will not be recognized.

Let me also make a few reminders to those members appearing in person. You will only see members and witnesses appearing remotely on the screens in this hearing room. On one side of the room you can see the individual who is speaking in what is known in Zoom as speaker view. On the other side you'll see the collection of individuals within the Zoom platform. A timer is visible in the room directly in front of you.

For members and witnesses

[inaudible].

I now recognize myself for an opening statement.

Since the enactment of the Federal Information Technology Acquisition Reform Act in 2014, this subcommittee has maintained steady and bipartisan oversight of the agency implementation of the law. FITARA was enacted to establish a long-term framework through which Federal IT investments could be tracked, assessed, and managed to significantly reduce wasteful spending and improve project outcomes. FITARA is a report card that holds agencies accountable and exhorts them to improve their IT postures, and in practice, it's a tool for Congress and the public to ensure better cybersecurity, reduce wasteful spending, and make government service to the Nation more effective. The coronavirus pandemic has proven that IT is integral, not incidental, to the mission.

As we have seen both at the Federal and state, local level of government, if the IT does not work, the mission does not work.

Today's hearing will discuss the results of Scorecard 11.0, which was released in December. This hearing will also focus on how Congress and the administration can work together to approve services to the Nation with a focus on improving IT across the government. Today's hearing also comes weeks after Congress was able to secure a billion dollars in the Technology Modernization Fund so that agencies have more opportunities to improve IT and enhance cybersecurity.

We look forward to engaging with the Office of Management and Budget about the importance of IT modernization and this funding opportunity at the next FITARA hearing in July.

Last summer marked the tenth FITARA oversight hearing in the last five years and the first time that all 24 agencies participating in the FITARA Scorecard received passing grades. Since the FITARA 10.0 Scorecard, three agency grades increased, five decreased, and 16 remained unchanged. Further, despite the removal and addition of metrics, all 24 agencies maintained passing grades for the second time in 11 Scorecards.

FITARA 11.0 marks the first—a few firsts in the five-year history of the Scorecard. The Scorecard marks the first time, for example, in FITARA's history that all 24 agencies included in the law received at least one A in a single metric. And that metric was the software licensing metric, the first time that metric will also be retired because everybody gets an A. When the subcommittee added this metric to the Scorecard back in June 2017, only two agencies had such inventories. Agencies needed a better management software licenses to make cost-effective decisions and to achieve savings.

As a result of continued oversight using the FITARA Scorecard, all 24 agencies are now using comprehensive, regularly updated inventories of the software licenses, enabling those agencies to identify duplicative licenses and software costs.

The GAO, the Government Accountability Office, estimates that agencies have saved or avoided more than $1.4 billion in software licensing costs from Fiscal Year 2015 through Fiscal Year 2020 because they are now using comprehensive, regularly updated inventories. These types of small but significant adjustments over the vast enterprise of Government can rack up significant savings pretty quickly.

FITARA 11.0 also marks the addition of a new metric which evaluates agencies' efforts to transition off the General Services Administration's expiring telecommunication contracts before they expire in May 2023. The new measure incentivizes agencies to progress toward telecom services that deliver critical services at lower costs to taxpayers.

Since the Scorecard's inception in 2015, agencies have made substantial positive strides in improving their information technology practices. Among the FITARA Scorecard categories with the greatest impact on taxpayer savings, of course, is the IT portfolio review process known as PortfolioStat. PortfolioStat went from helping Federal agencies save $3.4 billion in Fiscal Year 2015 to $22.8 billion at the beginning of Fiscal Year 2021. Let me repeat that. We

got savings of $3.4 billion back in 2015. Six years later, the savings are at $22.8 billion.

Federal agencies are closing and consolidating more data centers which also results and significant cost savings. The 24 graded agencies have reported more than $5 billion in cost savings in that category from fiscal years 2015 to 2020.

While the FITARA Scorecard has successfully help agencies move the needle on improving IT practices, work still remains. According to GAO, 21 of the 24 graded agencies still not have established policies that fully address the role of their CIO as required by Federal law and FITARA guidance. Improving the management of IT acquisitions and operations remains on GAO's high-risk list. Citing the need for OMB and Federal agencies to implement all of the statutory provisions of FITARA. Further in the most recent high-risk list, GAO reported that significant attention was needed to improve the Federal Government's management of IT acquisitions and operations and to ensure the Nation's cybersecurity.

The coronavirus pandemic has highlighted that chief information officers are more central now than ever before. Nearly every Federal program service and function relies on IT in order to work. It's among the duties of the CIO to plan for agency IT needs, including the resources required to accomplish the mission. Outdated legacy systems, software and hardware, however, continually prevent agencies from providing the services the American public expects and demands and deserves.

To determine the scope and feasibility of IT modernization, CIOs must be more involved in the agency performance planning. That's why today I introduce the Performance Enhancement Reform Act with my ranking member, Mr. Hice. This important piece of legislation requires agencies' performance goals to meet the demands of the ever-changing performance management landscape and includes data evidence and IT in their performance plan. The bill would also require agencies to publish their technology modernization estimates, system upgrades, staff technology skills and expertise, and other resources and strategies needed and required to meet these performance goals.

The subcommittee will continue to evolve the Scorecard in ways that facilitate tracking improvement over time, while adding new metrics as necessary to raise the bar on what is needed across the Federal enterprise. I look forward to today's important conversation so that we continue to provide accurate oversight and to exhort Federal agencies to come into the 21st century with their IT.

I now call my friend from Georgia, the distinguished ranging member, Mr. Hice, for his opening remarks.

Mr. HICE. Thank you, Chairman Connolly, and I appreciate your leadership on this issue and for holding this hearing today.

I likewise understand that the intent had been to invite the new Federal Chief Information Officer, Clare Martorana, but due to a family emergency, she is not able to be here. So, I certainly extend my sympathies to her and her family and look forward to working with her in the future as well and I understand likewise the urgency of holding this hearing but certainly regret the fact that we're not going to have the benefit of her views and hope we'll be able to have that at some point in the future.

That being said, FITARA no doubt has been a bright spot of bipartisan work for this committee /and I look forward to continuing those efforts in regards specifically to this Scorecard and its usefulness as it relates to IT reform in the future.

But while agencies have certainly progressed over the past five years, the task, as always, is to ensure that we are keeping the Scorecard current. We want to make sure that it's measuring the most relevant facets as it relates to the IT universe, and I look forward to the perspective of our witnesses today on how the Scorecard may potentially need to change as we continue going forward.

Since our last FITARA hearing in August, the Scorecard, as we all know, has been modified. It's gone—what is gone is the software licensing inventory required by the MEGABYTE Act and, as Chairman Connolly has mentioned, the agencies were receiving an A grade and that has been replaced by new category, Enterprise Information Systems. This is a new contract vehicle for agency telecommunications and will finally bring many benefits, I believe, including enhanced user experience and cost savings. My hope is that it will, in addition, drive agencies toward faster implementation, which has been a concern for many of us for a long time. We need to be able to meet the goals, not just have goals.

But there have been more important events since our last hearing than the Scorecard changes itself. Of course, the biggest has been the solar wind cyber-attack. This certainly reinforces the urgency to do everything we can as policymakers to keep Federal networks secure. That obviously is a major concern to all of us on both sides of the aisle.

In addition, a year has now passed since the COVID pandemic and the many multiple ways that it stressed agencies' ability to both operate and serve citizens in a remote digital environment. So, as we look to the future, gauging how we will accomplish these tasks, that certainly should be a top priority as well.

This goes hand-in-hand with the need to modernize aging legacy systems, also a very deep concern for many of us. These old systems simply are not able to manage the demands and expectations of Americans here in the 21st century. We've got to replace these legacy systems.

So, in closing, I do want to thank our witnesses who are here today. Thank you for taking your time to be with us. I'm eager to hear your insights and your suggestions and look forward to listening to your statements and to working with you as we move forward.

And so, again, thank you, Chairman Connolly, for your leadership in this area and this hearing.

And, with that, I'll yield back.

Mr. CONNOLLY. Thank you so much, Mr. Hice.

I'd like to introduce our witnesses today. We're grateful to have their expertise. Our first witness is Gundeep Ahluwalia who is the Chief Information Officer for the Department of Labor. Then we will hear from Jay Mahanand who is the Chief Information Officer for the U.S. Agency for International Development. And last but not least, we have Mr. Walsh representing the Government Accountability Office, which has been a great partner for us, and he

serves as the Director of Information Technology and Cybersecurity at GAO.

If the witnesses would be unmuted and raise their right hand and, Mr. Walsh, if you would stand and raise your right hand, it is the custom of our committee to swear in all witnesses.

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

Mr. AHLUWALIA. I do.

Mr. MAHANAND. I do.

Mr. WALSH. I do.

Mr. CONNOLLY. Let the record show all three of our witnesses have answered in the affirmative.

Without objection, your written statements, full written statements will be entered into the record.

And, with that, Mr. Ahluwalia, you're recognized for your five-minute summation of testimony. Welcome.

STATEMENT OF GUNDEEP AHLUWALIA, CHIEF INFORMATION OFFICER, DEPARTMENT OF LABOR

Mr. AHLUWALIA. Thank you, Chairman Connolly, Ranking Member Hice, and the members of the subcommittee for the opportunity to speak here today about IT at the Department of Labor. I want to thank DOL leadership and all DOL employees for their hard work and dedication in support of wage earners, job seekers, and retirees across the country. I also want to thank Congress for your continued support with FITARA and the resources for IT modernization as a whole.

As CIO, I have always strived to maximize available resources and apply them to an IT strategy, enabling data-driven decision-making and digitization aimed at better mission outcomes. FITARA's Scorecard helps show an agency's IT success, growth, and areas that may need improvement.

The Department's high marks in implementing FITARA is a testament to our organization's commitment to IT modernization. We are the only agency to receive A grades in six of the seven categories. As a result of our efforts in implementing FITARA and upgrading our infrastructure, Labor was able to quickly transition 95 percent of our work force to a remote work environment when the COVID–19 started, without any interruptions to mission delivery.

We maintained mission activities for 27 subagencies and onboarded more than 1,500 staff virtually. We continued to provide critical services for the American public, including protecting 401(k)'s, inspecting mines, ensuring workplace safety, and handling increased website traffic as people accessed weekly and monthly unemployment numbers.

It is important to note that investing in IT modernization is not a once-and-done scenario. During my time as CIO of the Department of Labor, our focus has been on paying down our technological debt, enabling the IT strategy, and utilizing the tools Congress has provided with FITARA, Modernizing Government Technology Act, and the Technology Modernization Fund. In addition to innovative contracting strategies, we are taking advantage of the

TMF funding opportunities coupled with our Working Capital Fund authority and appropriations for IT modernization.

For example, in 2018, we used the TMF funding to streamline the temporary labor certification program from a paper-based to a completely digital process, resulting in a $2 million annual—$2 million annual savings for the department. We are also centralizing IT, HR, and procurement functions, which has helped us avoid costs in the past and has positioned us to drive efficiencies in the future.

We are proud of the digitization successes we have achieved by modernizing our DOL websites to positively impact workers, employers, and the American public. For example, we developed apprenticeship.gov, a one-stop-shop website to bring together educators, employers, and job seekers to easily search for over 24,000 apprenticeship opportunities across the Nation.

And as referenced earlier, the temp labor certification process, DOL created a completely digital electronic boarding pass mechanism. By developing the system, we were able to reduce processing times and the need for manual printing and shipping.

The Department of Labor continued to move forward with its modernization efforts and has been successful in large part due to the funding mechanisms that Congress has enacted and supported. In fact, we are grateful to have received TMF funding for our enterprise data modernization initiative. This marks the second TMF award for DOL.

Thank you for your time today and your continued support to FITARA—for FITARA and IT modernization efforts. I look back—I look forward to answering any of your questions.

I yield back, Chairman.

Mr. CONNOLLY. Thank you, Mr. Ahluwalia, and you're a pro. You had, like, 49 seconds to go. So, thank you.

Mr. Mahanand, you are now recognized for your five-minute summation of item.

STATEMENT OF JAY MAHANAND, CHIEF INFORMATION OFFICER, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

Mr. MAHANAND. Chairman Connolly, Ranking Member Hice, members of the subcommittee, thank you for inviting me to testify today. I'm grateful for the committee's support, and I'm pleased to have this opportunity to discuss USAID's progress in complying with the standards set out in FITARA.

The global pandemic changed how we work, how we live, and how we interact with each other. For USAID and its people, responding to these global health crises is at the core of our mission. We have a longstanding history of dealing with emerging threats and global health security such as Ebola and now COVID–19. Because of this rich history, we were able to rapidly virtualize USAID's work force and leverage our leadership in cloud technology to lessen the impact on the agency's most valuable asset: its people.

USAID global IT infrastructure plays a critical role in enabling and enhancing every aspect of the Agency's mission. Our 12,000-plus people in more than 120 countries, often under the most difficult circumstances where communication capabilities are severely

limited, they depend on our cloud-based architecture to successful perform USAID's critical work. Because of this, we're an organization that relies on cloud services and solutions that enable data-driven decisions and maximize the impact of those efforts.

Now more than ever, reliable and secure and effective information technology systems and services are essential to USAID achieving its mission. As a global organization that works in some of the most challenging locations around the world and given the business demands of how USAID delivers U.S. foreign assistance on the ground, our overseas staff have been heavily reliant on modern and mobile IT solutions, even prior to the COVID–19 pandemic.

The move to a cloud-based email messaging and collaboration platform back in 2011 significantly and quickly improved USAID mission delivery. It provided a mobile, on-demand messaging platform that meets the needs of the Agency's global work force, improved cost-efficiency, enhanced cybersecurity and overall functional operational improvements to our IT environment. As early adopters, our leadership and staff across the agency are accustomed to working in a cloud environment, leveraging the cloud to underpin our communication, security, data, and development backgrounds.

Today USAID is 100 percent cloud-based with no legacy systems.

Given all that has transpired this past year, I think about where USAID was 10-plus years ago, where we are today, and what has helped us get here. Although our journey to the cloud began before FITARA and the Scorecards, the impact and benefits we have realized by its creation and evolution has significantly aided our journey. FITARA has served as a cornerstone for establishing, measuring, and helping advance critical IT programs for CIOs across the government. Our USAID's legislation has underpinned our success in aligning the people, processes, and technology needed to balance innovation with compliance, mission needs, costs, and evolving threats. It has also provided an opportunity to have a collaborative dialog with OMB, GAO, the committee, and Congress, working together to improve how agencies implement FITARA.

Although agencies will continue to face significant IT challenges and risks, this past year has shown the true benefits of a modernized, agile, innovative IT organization particularly during a global crisis. Aside from the technology challenges and moving thousands of employees to full-time telework overnight, the pandemic also ushered a new, more sophisticated way of cyber-attacks. As we have seen recently in the Solar Winds and Microsoft Exchange breaches, the threats are growing more pervasive, sophisticated, and damaging to both government and private sector organizations. As these threats become more advanced, the need for the Federal Government to further enhance its cybersecurity posture and better understand the various supply chains continue to grow.

Over the past year USAID has expanded its effort to leverage state-of-the-art technology, such as AI and RPA, to help the Agency realize the full potential within its many data sources. Each project represents a significant investment USAID is making in innovation tools and platforms that will continue to help secure our network

and data globally and help us keep pace with the Agency ever-changing technology and information needs.

USAID looks forward to the continued benefits the Scorecard and its measurement provide to Federal CIOs. Having consistent IT priorities across all agencies enhances mission outcome and provides a roadmap of technology investment that maximizes taxpayer dollars.

I would like to thank the Members of Congress, members of this subcommittee in particular, for your continued leadership, interest in, and support of our work. USAID looks forward to collaborating with you to address future challenges and new opportunities for reform.

Thank you for your time. I welcome your question.

Mr. CONNOLLY. Thank you. Thank you. And you had 30 seconds left. So, thank you.

I will say to you, Mr. Mahanand, a little piece of history you may not know. In 1979, when I got out of the graduate school, I was a Presidential management intern and I was offered a job at AID to help translate IT and policy. In that time cell phones didn't exist. The Internet didn't exist. Social media didn't exist. PCs didn't exist. It was a very primitive time. But can you imagine how history might have been different for you and me and my colleagues in this committee had I taken that job? Anyway, I'm glad you're there.

Mr. Walsh, welcome again, and you are recognized for five minutes for summation of your testimony.

STATEMENT OF KEVIN WALSH, DIRECTOR OF INFORMATION TECHNOLOGY AND CYBERSECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WALSH. Chairman Connolly, Ranking Member Hice, members of the subcommittee, thank you for inviting GAO to testify on this important issue today.

To begin, I'd like to share one of my favorite Scorecard-related quotes from the chairman who has repeatedly said that the Scorecard is not intended to be a scarlet letter. Rather it is intended to start a conversation and to make sure that CIOs are part of that conversation. Regardless of the letter grades on the Scorecard itself, I think that elevation of our agency CIOs may be the most impactful effect of the committee's oversight. So, thanks to you and to your staff for your continued contributions to and oversight of Federal IT. Your persistent, thorough, and bipartisan oversight has changed the way the government manages its technology.

Here are some key highlights of the progress that we have seen. Major increases in the authority for the five CIOs that now directly report to the agency header deputy; minor, but no less important, increases in the authority and influence of all CIOs, largely due to the attention the Scorecard has brought to the role; and better management of agencies' IT portfolios to the tune of $22.8 billion saved.

As the chairman noted, the most recent 11 Scorecard introduced two significant changes. First, the committee sunset the area related to software licenses. When the committee added this area in 2017, there were just two agencies that were using comprehensive,

regularly updated inventories of software licenses. Now all 24 agencies do, resulting in a number of easy A grades for the past several Scorecard cycles.

Second, the committee added a new area related to agencies' efforts to transition off GSA's expiring telecommunications contracts. This area needs the committee's oversight because the last time the government went through a similar transition onto the network's contracts, the government took 33 months longer than planned. It resulted in $66 million in added costs and an estimated $329 million in lost savings.

As you might expect, replacing the easy A of software licenses and the addition of the area on telecommunications transition put downward pressure on agencies' grades. Despite this, every agency passed by either receiving a B or a C. That may not always be the case. Agencies' past wins are no guarantee of future success, and the Scorecard reflects that.

The Scorecard's continued growth has kept it relevant, and it will be an important tool for keeping Federal leaders accountable going forward. For example, the Scorecard could measure Federal websites' compliance with industry best practices in conjunction with the IDEA Act. It could also reward or give a bonus to the usage of the billion dollars recently received by the Technology Modernization Fund.

However, the Scorecard is only as good as the data behind it. In that vein, it would be great to see OMB's IT dashboard reflect more of the government's IT spending. For example, right now, the dashboard does not include IT spending related to weapons systems, satellites, or supercomputers. The government's budding efforts to implement Technology Business Management, known as TBM, may help in that regard by closely linking agencies' accounting systems to IT oversight. However, half measures or an implementation that mimics true TBM will perpetuate the underreporting of IT spending.

I should also note that the Scorecard is not a panacea. There are many critically important topics that are difficult to implement and grade and address: for example, measures of how well an agency serves the citizens, an agency's human capital skills and gaps, or even the IT acquisition cadres and strategic sourcing required under FITARA. Metrics on softer topics such as these are incredibly difficult to measure. How well has USAID's technology served our farmers or the IT and IRS our taxpayers? Has the DOD protected our citizens enough?

These gaps also stress the significance of the work done by public servants who, regardless of the Scorecard's grades, do incredible work. These gaps in coverage also underscore the importance of having trusted, competent IT leaders and ensuring that they are a part of conversation.

To that end, I look forward to our continued conversations and the improvement of IT oversight. This concludes my comments, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Mr. Walsh, also, 30 seconds.

I mean, we've got three stars this morning, Mr. Hice.

The chair now recognizes the distinguished Congresswoman from the District of Columbia, Eleanor Holmes Norton, for five minutes of questioning.

Ms. NORTON. Thank you very much, Mr. Chairman. Chairman Connolly, I very much appreciate these periodic hearings.

My first question is for Mr. Walsh. The Federal Government currently invests about $90 billion annually in IT. Now what troubles me is that a third of the funding dedicated is for maintaining legacy systems. And so, what we're finding is that, as the amount of dedicated funds to IT operations and maintenance increases each year, the investments in the innovative IT projects decline.

So, Mr. Walsh, my question to you is, how do the current budgeting and appropriations cycles—and we understand that's done on an annual basis—impede agencies' ability for investing in critical IT projects, especially ones that concern me, that seek to replace legacy systems? Is there anything we can do about it?

Mr. WALSH. So, the annual appropriations process——

Mr. CONNOLLY. Mr. Walsh, I am going to—you are soft-spoken. If you would move that as close to you as possible, thank you so much.

Mr. WALSH. Thank you, chairman.

So, the annual appropriations process certainly does not help our efforts to modernize Federal IT. Having to save up multiple years to address a critical need is not currently possible. The MGT Act a few years ago attempted to address that by allowing agencies to save money in a Working Capital Fund and use the savings to address cybersecurity and modernization needs. So, I think that's a good step forward. However, the MGT Act did include a critical flaw that has prevented many agencies from fully taking advantage of those flexibilities.

Ms. NORTON. I can see that the problem's in the Congress.

Mr. Walsh, several of the agencies have said that the reimbursement model itself is cumbersome, especially for IT projects that are critical to the mission but might not realize costs. What other considerations should Congress, and the administration take into account, other than projects that realize hard costs?

Mr. WALSH. So, as you correctly note, there are many, many, many things that we should consider when modernizing legacy systems. In particular, the functionality is very important. But there are also very, very old systems that cannot be modernized. For example, we wouldn't want to modernize the Voyager space probe's ground systems. We can't modernize the Voyager. It's out past the edge of the solar system at this point.

But the cost and the functionality are crucial, and in many cases, modernizing systems cannot result in cost savings. The new systems that we're using right now in the cloud have a lot better capabilities. They have a lot better security than some of these very, very old systems.

So, you correctly note that, in many cases, we may not save costs doing modernization, but it would be better for the services of our taxpayers to do so.

Ms. NORTON. Thank you.

Finally, Mr. Mahanand, could you talk about your experience with establishing an IT capital fund at USAID?

Mr. MAHANAND. So, that has been an ongoing issue for the last three years for us. We've actually worked very close to OMB, our examiner and senior level, senior leadership within the agency. They are all very supportive as far as getting—putting the language together and getting us to at least get it into the President's request, but as far as what happened there, we're not necessarily sure. We actually included it in the 2019, 2020, and 2021 budget requests. But it never made it into any of the appropriations.

Ms. NORTON. My time is close to expire. I had another question. But thank you very much, Mr. Chairman.

Mr. CONNOLLY. If you have one more question, Ms. Norton, you're free to ask it.

Ms. NORTON. Yes. Mr. Ahluwalia, how can technology, the Technology Management Fund, which was established by the Modernizing Government Technology Act, which received $1 billion, and the American Rescue Plan, has that helped the Department of Labor accelerate certain IT modernization projects?

Mr. AHLUWALIA. Thank you, Congresswoman. So, I'll try to be really very quick here.

We are one of the few agencies who has received two TMF awards from that board, and it is a toolset that we use in conjunction with our appropriations Working Capital Fund authorities to resource and modernize technologies. I am very proud of one of recent temp worker program. The visa requires a labor certificate from DOL that used to be printed on a currency-like paper, and I shudder to think what would have happened to that printing operation during COVID–19. Fortunately, this January, in part due to the TMF funding, we were able to completely digitize that process and shut down the printing operations, which has now resulted in a $2 million savings that will be returned to the fund.

I do agree with my colleague, Kevin Walsh. Not every—when you replace a bicycle with a motor car, will it result in savings? The motor car will require sometimes more to maintain, but it takes you farther and faster. So, that construct has to be considered in the future mechanisms when the DMF awards are made.

Mr. CONNOLLY. Thank you very much.

Thank you, Ms. Norton.

The chair now recognizes the distinguish ranking member, Mr. Hice, for five minutes of questions.

Mr. HICE. Thank you, Mr. Chairman.

Yes, the challenge of any effort like FITARA at the end of the day is to prevent it from going stale. I think, when we are trying to ensure Federal IT funding is spent well, the most obvious question is whether there are metrics to determine whether or not that money is spent well and how we gauge it. So, let me start with this train of thought.

Mr. Walsh—and we spoke a little bit about this before the hearing this morning. But given the fact that this is the 11th iteration of the Scorecard, what changes perhaps need to be considered by the committee to deal with the metrics to make sure we're being effective?

Mr. WALSH. So, to the Scorecard's credit and to the committee's credit, it has changed in every single iteration since the second. Every single time the committee has made sometimes minor but

important tweaks to improve this Scorecard. This most recent 11 Scorecard is an excellent example of some of the changes that can be made with the sunsetting of the software licensing and the adding of EIS. So, it's a credit to the committee that this Scorecard continues to evolve and change.

To get closer to how to evaluate the efficacy of how the government is spending our money is a very, very difficult concept, sir. I think the Scorecard is helping move us in that direction, but measuring how good an agency is at delivering its mission or meeting its mission is something that we in the GAO and Congress have struggled with for quite a long time.

Mr. HICE. Well, is there any way we can quantify the return on investment through 11 scorecards so far?

Mr. WALSH. So, the $22.8 billion that have been saved or avoided as a result of the PortfolioStat initiative is one very, very large metric we can use to measure ourselves. The increases in CIO authorities are also important but harder to quantify.

Mr. HICE. I would like to see more of that on a page, like, how do we really know there's this much savings, and where is that savings coming from?

You mentioned in your opening statement the Solar Winds and several—a couple of our witnesses did. Again, the metrics of something like solar wind in the Scorecard, how do we develop that to better equip Congress to recognize problems and deal with problems before they happen?

Mr. WALSH. So, part of the challenge when deliberating with you folks on how to come up with these metrics is what data are currently available. Especially in the case of supply chains, we want to be careful not to utilize nonpublic data. We don't want to put a target on any agency's head that's not already there. I agree that supply chain management and the risks associated are critically important to cybersecurity and our government's operations, and we would love to work to explore further metrics that we can use to measure that. I think a note of caution is warranted though with things as secure and sensitive as that.

Mr. HICE. Let me cast that question over to Mr. Mahanand and Mr. Ahluwalia. As it relates to the cyber issue, the cyber-attacks, No. 1, I guess, what keeps you both up at night? And what can we do on this thing and on our side as it relates to the Scorecard to better assess where we are on the cyber-attack concern?

Mr. Mahanand?

Mr. MAHANAND. Yes. So, I think we're on a good path here. If you actually look at the cybersecurity metrics that you have on the Scorecard, half of it is about cross-agency priority goals, which is something that the agency—the Federal Government can decide, know exactly how they want to measure that. But the other part of that is really it comes from the audit of your system or the audit of your network. And as far as that audit is concerned, it does take a close look at really the controls that you have in place in terms of your systems. And it gets to whether, you know, you are doing well in cybersecurity, where you're actually monitoring and managing it, or you're not doing so well in it.

I think that's a really good start because in the new version of the kind of the audit document here, they're going to be looking at

supply chain controls for the next, you know, assessment period here. So, I would think that, as far as the metric is concerned, I think it's a good place to start. You can also incorporate more into that as far as the cross-agency goals or as far as the audit is concerned.

But this is something that I know it is becoming more visible. I just think this year the audit is possibly going to be looking at supply chain and controls the agency may have in place. So, I think you will get some better, you know, better data when the audit is complete or the next Scorecard is put out.

Mr. HICE. OK. Mr. Ahluwalia—I'm sorry—if you could provide us an answer with that, I'm really curious. I mean, you are among our experts, and I'm curious how we can be better informed as Congress when it comes to the cyber threat. So, if you could provide an answerfor us in the next week or so, I would appreciate that.

Mr. AHLUWALIA. Happy to do that, Congressman Hice.

Mr. HICE. Thank you. I yield back.

Mr. CONNOLLY. I thank the ranking member.

The chair recognizes himself for five minutes.

Mr. Walsh, what is a legacy system?

Mr. WALSH. So, legacy means many things to many different people.

Mr. CONNOLLY. I have got to hear you. You have got to speak up.

Mr. WALSH. Legacy means many things to many people, sir. I think probably one of the better definitions is something that is no longer vendor supported, whether that be hardware or software. So, if the vendor's not supporting it, if we're not able to easily maintain it, I think that's an easy definition of a legacy system. Similarly, you could say something along the lines of what DOD does, that a legacy system is a system that no longer meets its mission needs. So——

Mr. CONNOLLY. Are we concerned that, under either of those definitions, legacy systems cannot be encrypted to protect from cyber hacking, cyber attacks?

Mr. WALSH. Absolutely, sir. And I think that's one of the things we saw at OPM when they had that breach a few years ago. One of the things that came out of that was we heard that OPM was not able to encrypt the data that was on the servers at rest because of the age of the systems.

Mr. CONNOLLY. I think that's a pretty critical point to be emphasized.

Are agencies required, Mr. Walsh, to have a plan to retire or upgrade legacy systems?

Mr. WALSH. So, we did work on this a few years ago, sir, and we looked at the most important and the most critical systems in the government to be retired, and we found that in many cases not only were they not required but they did not have plans and those plans did not include things like a description of the work to be done, milestones, or a plan, most importantly, to turn off the legacy system that they're retiring.

Mr. CONNOLLY. From GAO's points of view, think, putting on your high-risk category hat, would it be helpful if, in fact, they were required to have such a plan?

Mr. WALSH. I think we should absolutely be thinking about the oldest systems in need of modernization and have some form of plan going forward on how to either turn it off or get it to a more secure space.

Mr. CONNOLLY. Has GAO done any kind of cost estimate? On just, you know, spit-balling, if we were to have by fiat all legacy systems need to be replaced and you need to have a plan to do that, what would it cost across the 24 Federal agencies we're looking at?

Mr. WALSH. We have not done that work, sadly, sir. We did have some case studies in our report that looked at some of the most important, for example, one of the top 10 was—and we did not name these systems but it was at the IRS. IRS spent $10 million per year to operate and maintain the system, and their estimate on how much it would cost to modernize the system was $1 billion.

Mr. CONNOLLY. Billion.

Mr. WALSH. Billion.

Mr. CONNOLLY. With a "B."

Mr. WALSH. So, to Mr. Hice's earlier comments, the return on investment there would be somewhat dubious.

Mr. CONNOLLY. Well, yes, although every dollar you're invested in the IRS has a return on it. It's not a sunk cost.

Mr. WALSH. Absolutely. You've got the $40 billion that——

Mr. CONNOLLY. By the way, that's true for your agency as well. We get a return on our investments with you and your colleagues at GAO. So, we have to think it in those terms, too. And as you pointed out, then there are the sort of imponderable or indecipherables. But they're still so important, right, like quality of service to the American people. That kind of matters, too.

Let me ask about CIOs. How, from GAO's point of view, when you're looking at the Scorecard, how much progress are we making or not making in having a premier CIO report directly to the boss?

Mr. WALSH. So, since this first Scorecard, we now have five more CIOs that directly report to the boss. We also have seen incremental progress elsewhere. It's a lot harder to measure which CIOs have a seat at the table that they did not previously have, but those five CIOs having reporting authority I think is the most important metric there.

Mr. CONNOLLY. We've had—have we had some backsliding in that regard?

Mr. WALSH. To the best of my knowledge, I am not aware of any agencies that are backsliding I think in large part due to the attention brought by this committee.

Mr. CONNOLLY. I mean, you know, if you look at the private sector, I can't think of many successful companies where the CIO does not directly report to the CEO and even dotted-line relationships in the organizational chart don't count, and we've got to evolve to a system where the CIO, because if we really mean it about fundamental changes in IT modernization, in order to undergird the mission, we've got to have a CIO who's empowered. And the best way in a bureaucracy to empower somebody is to make sure everyone can see that person reports to the boss.

Mr. WALSH. Absolutely, sir. It's hard to imagine a company these days that does not have IT-involved core to its mission. Similarly,

it's hard to imagine a government agency that does not have IT contributing critical amounts to its mission.

Mr. CONNOLLY. And final question in this round, we just got $1 billion for the Technology Management Fund, which is not what we wanted or what President Biden wanted. But it's certainly a huge quantum leap from what was appropriated at $25 million. Do you believe that that $1 billion will be a significant catalyst to incentivize agencies to make the investments we're talking about including the return of legacy systems?

Mr. WALSH. So, previously the fund was receiving $25 million per year, as you noted. Getting $1 billion in a year is going to allow them to explore projects that were previously outside of their ability. They didn't have the money to address some of these most critical needs. So, I think it will be important. The challenge is going to be ramping up that team that manages the TMF to make sure that they have the expertise necessary to oversee these projects.

Mr. CONNOLLY. Yes, I also think we're going to have to have clear criteria soon because the expectations are really high about this. We're going to have to have criteria soon from OMB in terms of how that fund could be used and how it should be used. And we're going to hope GAO is monitoring that carefully so that if there are real-time issues, we can try to address those in real time rather than retrospectively because then the damage is done.

Mr. Hice, who is to be recognized?

Mr. Keller is recognized for five minutes.

Mr. KELLER. Thank you, Chairman Connolly. And thank you to the witnesses for taking time to be here today.

The pace of government often lags behind that of the private sector, and the process of technology acquisition is no exception. As agencies struggle to keep up with current technology, Federal acquisitions often overshoot their targeted time and cost estimates. Along with ensuring cybersecurity and transparency, the Scorecard should measure how effectively an agency is purchasing and utilizing new technology. My time in private industry, our mentality was that the team I worked with could not improve unless we knew exactly how well we were performing and what targets we were hitting. The same should go for Federal agencies.

The question I have is for all the panelists here today. Part of Congress' job is ensuring Americans get the most out of their tax dollars. How does FITARA achieve this end? And are they—and are there any modifications to FITARA that would help us better capture this metric? And that could be for anybody. Maybe all the panelists can give me a little bit of explanation of what they think.

Mr. CONNOLLY. Mr. Keller, without prejudice to your time, are you asking modifications to the Scorecard or to the underlying legislation itself?

Ms. KELLY. The Scorecard.

Mr. CONNOLLY. Yes. Thank you.

Mr. AHLUWALIA. So, I'll go first. This is Gundeep. I'm the CIO for the Department of Labor.

I think the ability to use various types of resources is, that span across multiple years is an important mechanism and a differentiator in the way government and the private sector works. So, I look back at my private sector years and on what the dif-

ferences are. One is these projects are multiyear, and we try—and we don't have the visibility for the resources on that. Having a clear plan that has outcomes not about moving to the cloud or about taking software out—those are important as well—but having outcomes like I will remove paper from a labor certification process or digitize it completely or I'll reduce the number of—reduce the number of days that it takes for a person to consume its service from the government, or I will make it mobile friendly like the private sector. You can go to Amazon and sort of have that shopping experience and that kind of customer experience.

Those are the metrics that we focus on to bringing the services that we render to our constituents at par with the private sector. And a focus on that, managing resources as a multiyear resource and with a strategy to execute to, those are the key ingredients that I remember worked in the private sector and would work in the public sector as well.

Mr. KELLER. So, as far as modifications to FITARA that would better capture the metric, I understand how we want to do it better. But, again, any other thoughts from the other witnesses?

Mr. MAHANAND. This is Jay Mahanand, USAID CIO.

So we—as you can—from my testimony, you can see we've actually moved quite a bit of innovative technologies, you know, that we've implemented or started. For instance, really looking at, you know, how we can get started, I think that's the key to anything we do. But whether or not a technology is viable for an organization, that's something to be said and something we need to go through.

For us, we're—an example is that we're very intensive when it comes to data and so, you know, questions in terms of all of the data that we have, what do we do with it, and how do we make it—you know, how do we use technology to actually innovate and be able to get answers on the raw data there. So, for us, it's really just taking, you know, some time off and basically create a pilot, some use cases, initiate those use cases with the technology that we have, and try to validate whether or not that is something we can go.

But for us is that, given the fact we don't get a large amount of money, we simply use, you know, kind of the prototyping to kind of make a determination whether or not the technology would work for us. And so we've been pretty successful because if we can show the agency that, hey, this provides or brings value into the organization, then there's always funding that is, you know, that would be subsequently, you know, coming for that specific technology.

So, I think that's how we do it internally because we always look at something. And even I mentioned, you know, robotic process automation, in terms of efficiency that it gains because, you know, there's quite a bit of just manual process we have in agencies. We talked about doing more for less. That is the way that we see things and how we would actually get things started. Technology has been in place. But we need, you know, the people, processes, and technology all to work together. So, we pilot certain things to make sure that there's an appetite for those types of technology in the agency because there's an adoption. There's also change-manage-related issues to bringing technologies in place as well.

So, it's a complex discipline in terms of how you would measure that. You know, for me, kind of getting back to, you know, some of the comments that were made, you know, specifically when it comes to, you know, ROIs and, you know, getting money to actually make a determination of how technology would be used, the TMF is a good example of that. We kind of—it has been mentioned that, you know, for us, we actually made proposals in the TMF for a couple of—we would say innovation, and we got declined for that because it was more—not necessarily a modernization but also it was toward innovation.

So, I think, on the TMF, my two cents is also not look just at modernization but, getting to your point, really is take a look where agencies can use that money to innovate and be better at that.

Mr. KELLER. Thank you. I see I'm out of time, so I yield back.

Mr. CONNOLLY. Mr. Keller, I will certainly entertain Mr. Walsh if he wishes to respond to your question before you yield back.

Mr. WALSH. Sir, one of the ways that we could perhaps better measure how we are serving the citizens is how well their websites, which, you know, is the prime portal that people interact with, citizens, are compliant with best practices, are enforcing privacy metrics. So, that is something that we would love to explore with the committee and look forward to doing so.

Mr. KELLER. I appreciate that. Thank you.

Mr. CONNOLLY. And, Mr. Keller, we can talk to you offline, but I believe we have some legislation that actually addresses trying to upgrade websites and make sure they're user-friendly and that they're ranked and reviewed. So, that's absolutely—because that's the portal for most citizens to the government, at least electronically.

Mr. Hice, is Mr. Biggs the next one? Yes. Mr. Biggs is recognized for five minutes.

Mr. BIGGS. Thank you, Mr. Chairman, and I thank the witnesses for being here today, for sharing their perspectives on this critically important topic.

Like many of my colleagues, I was especially disturbed by the early 2020 Solar Winds hack, which left nearly 20,000 entities vulnerable to data breaches, including the Departments of Defense, State, Energy, Justice, and Treasury in the public sector, and Microsoft, Cisco, and FireEye in the private sector. Amazingly, that attack happened over the course of more than a year, which showed a chilling level of patience and discipline.

So, my first question—and it's for each member of the panel—is this: How confident are you that we are better protected from a drawn-out, solar-wind-style attack now than we were in early 2020?

And I'll start with you, Mr. Walsh.

Mr. WALSH. So, we had a remarkably timed report at the same time as the Solar Winds hack, GAO 21–171, which looked at agencies' implementation of supply chain risk management.

We looked at seven key practices identified by NIST guidance that attempted to help agencies manage those risks. We found that only nine agencies had done any of those seven. So, to your point, sir, I think we should be very concerned.

Mr. BIGGS. Please, the other panelists, please respond as well. Thank you, Mr. Walsh.

Mr. AHLUWALIA. So, at Labor——

Mr. CONNOLLY. Would my friend just yield for one second and without prejudice to——

Mr. BIGGS. Yes. Yes, Mr. Chairman.

Mr. CONNOLLY. Just to followup on that. Could it have been avoided? I mean, you said we need to be very concerned. Well—but could we have stopped it, done something about it?

Mr. WALSH. So, one of the seven practices that we identified is helping to detect problematic items in your supply chain. But, backing up it even further than that, part of the issue is knowing what your supply chains are.

There are many agencies that don't fully know what their supply chain, not only of the hardware but also of the software, is. So, I think could we have prevented it? Probably not at that time. It's disappointing as well that it took so long to detect it. So, it's very, very concerning, sir.

Mr. CONNOLLY. Thank you for yielding.

Mr. BIGGS. You bet, Mr. Chairman.

And I—just so you know, Mr. Chairman, I intend—if there is time, I want to followup with what's happening now and the steps that are being taken.

So, would the other panelists please respond.

Mr. AHLUWALIA. So, at Labor, just like other departments, we take the cybersecurity very seriously. I think the DHS' Continuous Diagnostics and Mitigation Program, the CDM program, has had significant impact and probably protected us from that breach when it happened.

We've implemented a 24/7 SOC. We are meeting—and implemented newer technology as well.

I completely agree with my fellow panel members here, as well as the committee, that the supply chain risk remains one of the largest risks that is there to the entire U.S. economy, in the private sector as well as public sector.

From the public sector perspective, it is my thinking that there are some steps that can be taken in individual departments. For example, understanding what our supply chain means, adding language to our contracts, and things of that nature.

But then a more comprehensive approach, looking at the CDM success, I think can be led by DHS. That crosscuts and protects the entire government apparatus rather than piecemealing it at each department at a time.

So, I think there is a combination of a strategy where some steps need to be taken locally within the departments, and then a comprehensive CISA-, DHS-led strategy to protect our apparatus would be the biggest bang for the buck, Congressman.

Mr. BIGGS. Thank you. And then our last panelist, if you could please be brief because I want to get back to what are we doing now, how are we going to get——

Mr. MAHANAND. Yes. So, just to—the one thing that we need to realize is that this is a cost application that was vulnerable, right? And so one of the things that we really need to look at is the supply chain. But, also, how do we extend some of the cybersecurity

measures to these specific vendors? And it's something that we need to think about.

I know DOD is looking at the cybersecurity certification for vendors, but that is something within the Federal space we know—we have risk-management frameworks. We have cybersecurity frameworks. We have everything to protect our systems in C.

The ability to, you know, implement zero-trust—zero-trust architecture is something that we are all looking to do. But the point still goes back to we still need to do something with the vendors to make sure that there is some sort of certification that they also validate the supply chain.

Thank you.

Mr. BIGGS. Thank you.

Mr. Walsh, would you please respond to the followup question, which is where are we going——

Mr. CONNOLLY. Mr. Biggs, if you had a brief followup, you're recognized for that.

Mr. BIGGS. Thank you, sir.

Mr. Walsh, if you'd just go to the followup, which is where are we going from here?

Mr. WALSH. Sure. So, I think the best practices that we can implement are detailed in the report I cited earlier, which is, as Mr. Mahanand said, getting some idea of what our supply chains are and working closely with the vendors to make sure that we are securing them.

Having executive oversight is also very critical. But, to sound an alert on where we are now, the Cybersecurity and Infrastructure Security Agency has issued multiple alerts over the past several months citing similar things happening with, for example, Microsoft Exchange, or even our critical infrastructure—the water, power plants, and the like—which were vulnerable to attacks.

Mr. BIGGS. Thank you, Mr. Walsh.

And thank you, Mr. Chairman. And I hope that, in the future, we might have an additional time where we can actually expand on this particular topic even further.

Mr. CONNOLLY. Absolutely. Be glad to work with you on that, especially, frankly, the—Mr. Walsh's insight in terms of supply chain. I think that's really—we need to understand that more than the phrase, right? Like, are we talking hundreds of parts? Because, if that's the case, no wonder somebody could penetrate, because——

Mr. BIGGS. Right.

Mr. CONNOLLY [continuing]. how are we monitoring all that. What are the mechanisms for monitoring all of that?

Mr. WALSH. Sir, it's not only the parts, but it's also the software. Every single piece of cloud software that we have installed on the network is potentially——

Mr. CONNOLLY. No, no. I'm including that in the supply chain. And, I mean, when I heard that, it—my ears perked up. So, we'll followup on that, Mr. Biggs, with you. Thank you so much.

We're joined by the vice chairwoman of the subcommittee, the gentlelady—and I know it's early out there in California, so thank you so much for joining us so early. Ms. Porter is recognized for five minutes.

Ms. PORTER. Thank you very much, Chair.

Mr. Walsh, can you briefly tell the committee what a data center is?

Mr. WALSH. So, currently, OMB defines a data center in two different tiers. A tiered data center is essentially something that you probably picture when you hear the word data center. It was purpose built. It has uninterruptible power supply, cooling solutions, and the like.

There is also what OMB categorizes as a nontiered data center, which are getting less attention, but those are things like servers in smaller rooms that were not purpose built but are still important vectors of bad actors trying to get into our agencies.

Ms. PORTER. I understand that there is a data center operation initiative. What is it meant to do exactly?

Mr. WALSH. So, the data center optimization initiative is intended to help our data centers, the big ones that already exist not only consolidate but get better. So, we want them to utilize more of their capacity. We want them to run on more modern hardware, which can save us operational costs, and make sure that we're best using the tools that we have available to serve our citizens.

Mr. CONNOLLY. Could I interrupt one second, Ms. Porter——

Ms. PORTER. Of course, sir.

Mr. CONNOLLY [continuing]. on that point? I want to stress the law, FITARA, refers to data center consolidation. It does not refer to optimization, a phrase that was invented by OMB and OPM that we were—this subcommittee, on a bipartisan basis, was concerned could be used to actually circumvent the requirement of the law.

And, Mr. Walsh, before Ms.—without prejudice to Ms. Porter's time, could you just address that because that remains a concern of this subcommittee. The law must be complied with, and the law says consolidation, not optimization.

Mr. WALSH. Absolutely, sir. And I think my fellow witnesses here might be able to serve very well in terms of what the current state of their data centers are, how many they have left. But you are absolutely correct. The law says consolidation, and we still want to see agencies closing and consolidating those data centers. We don't want empty data centers.

Mr. CONNOLLY. Right. So, in response to Ms. Porter's question about what is this optimization initiative, that is what? In addition to the requirement of the law?

Mr. WALSH. Sir, the law is the law.

Mr. CONNOLLY. Well, I know that.

Mr. WALSH. Yes. So, OMB's data center optimization initiative, yes, it is in addition to FITARA.

Mr. CONNOLLY. OK. It's in addition to.

Thank you, Ms. Porter. I wanted to clarify that.

Ms. PORTER. Absolutely. Thank you very much, Mr. Chair.

So, in the past, the GAO has testified before this committee that data consolidation not only protects us from cyber-attacks, but it also decreases cost to taxpayers. In fact, Mr. Ahluwalia—I'm going to mess up his name—Ahluwalia. How did I do? Slow.

Mr. AHLUWALIA. Excellent, Congresswoman.

Ms. PORTER. In fact, Mr. Ahluwalia, how much has the Department of Labor realized in cost savings through closing 73 data centers?

Mr. AHLUWALIA. Thank you, Congresswoman.

I think this is one of the bright spots of our portfolio and how we have been able to realize savings. Over the last few years, we have been able to close down 73 of these data centers, and despite what the regulations are and the current initiative status is, we are tracking every tiered and nontiered data center. We have saved around 70-plus million dollars, to answer your question directly.

Ms. PORTER. Thank you. So, you were able to save over $70 million and able to reduce office space, consolidate contracts and services, cut duplicative costs.

Mr. Walsh, do you know how much agencies in total have saved because of the initiative?

Mr. WALSH. I do not have the numbers at hand. It is in the order of billions of dollars.

Ms. PORTER. What I have is total of about $7.1 billion in savings, either cost savings or cost avoidance, for fiscal years 2012 through 2020. Clearly, this metric has prompted some pretty big savings for taxpayers.

But, in June 2019, the day before the FITARA 8.0 hearing, the OMB issued guidance updating the data center initiative. They redefined and narrowed the definition of a data center in a way that, according to the GAO, eliminated the reporting of over 2,000 facilities governmentwide.

So, Mr. Walsh, if we leave out more than 2,000 facilities, we're missing out the evaluation and potential, you know, improvement and cost savings of all of those facilities through this effort. Isn't that right?

Mr. WALSH. That is correct.

And to Mr. Ahluwalia's point earlier, he mentioned that they are tracking not only the tiered but also the nontiered data centers. Tracking the nontiered data centers, those are the ones that fell off. That's the 2,000 that you mentioned there. So, it's, in a sense, the——

Ms. PORTER. And those are those smaller ones that weren't necessarily intended to be data centers, those nontiered ones. This could open us up to cyber-attacks, couldn't it?

Mr. WALSH. That is correct. And we have encouraged the OMB and the agencies to continue their tracking of these nontiered data centers.

Ms. PORTER. That's potentially wasting taxpayer dollars, because we're not evaluating these nontiered data centers for potential consolidation or optimization?

Mr. WALSH. That is correct. And to help put a face to the name, some of these smaller data centers include things like FAA's air traffic control centers or large medical machinery that has basically supercomputers built into it.

Ms. PORTER. I'm pretty concerned about those things, FAA data and medical data.

Thank you very much, Mr. Walsh.

At every hearing since OMB issued this rule, members of this subcommittee have brought up the data center definition issue. It seems from these hearings that OMB thinks it's following appropriate private-sector best practices. And GAO thinks that we're exposing cyber insecurities.

Has GAO been working with OMB to ensure Federal agencies are not turning a blind eye to potential cybersecurity risks or wasting tax dollars?

Mr. WALSH. So, we do correspond very closely with OMB. We work with them as best as able. So, we try. And we do have annual reporting requirements——

Ms. PORTER. Mr. Walsh, are they listening to you, or are they ignoring you?

Mr. WALSH. I would say it's a push-pull. We work as collaboratively as we can, but sometimes it does feel like it's more of us talking and them not listening.

Ms. PORTER. But I get the sense, Mr. Walsh, that you're doing the pushing and the pulling, and they're doing the resisting. Is that an incorrect takeaway?

Mr. WALSH. So, there are times that we have worked very collaboratively, and I do not want to disrespect OMB or the good work they do. But, on certain issues, we don't always see eye to eye, so I think you're correct.

Ms. PORTER. Are they currently—with the GAO in its professional opinion—again, respecting the mission of OMB and the work that they do, is OMB in compliance with FITARA?

Mr. WALSH. So, I hesitate to come out with an official GAO opinion on this just because, right now, with the administration change, we have not yet seen how they are going to treat this issue.

Ms. PORTER. OK. Well, I look forward to finding out what you find in the post-administration change.

So, I think we're really right that we need to consider potential solutions, not just letting you do the investigation under the new OMB management, but I also support a potential legislative fix if OMB continues to not follow through. If they're not following the statute or they're defying congressional intent, then I think we need to consider legislation or even enforcement action.

Thank you very much for sharing your expertise with the committee today.

I yield back.

Mr. CONNOLLY. Thank you, Ms. Porter. And I love your spirit because I feel the same way.

You don't get to come into compliance with FITARA by redefining what a data center is, and you don't get to come into compliance by actually substituting a word in the law with another one that suits your purposes better and gets you off the hook.

And we are going to insist on compliance with the law. And, if we have to—as Ms. Porter suggests, if we have to further refine legislative language to make it very clear and, unfortunately, more restrictive, we will.

And we certainly will back up your efforts, Mr. Walsh, and those of your colleagues to insist on compliance. Let there be no doubt about that.

We are joined by the distinguished ranking member of the full committee, Mr. Comer. Mr. Comer, welcome. You're recognized for five minutes.

Mr. COMER. Thank you, Mr. Chairman.

I have a couple of questions for Mr. Mahanand and Mr. Ahluwalia. I mispronounced that. But since most people now expe-

rience government through digital interactions, an agency's IT system is critical in building citizens' trust in their government, obviously.

How does your agency measure the digital experience that you are designing in your IT systems?

Mr. AHLUWALIA. So, I can go first, Congressman. Thank you for the question.

At Labor, the service that we provide to the constituents that we serve is extremely important for us. So, the—one of the discussions earlier was around IDEA Act and compliance with it. We have taken that—the implementation of that act very, very seriously.

We developed a one-web initiative, where we have instituted the responsive design parameters that the private sector uses, and also made all our websites mobile friendly and accessible for the general public. The mobility as well as the user-centric design of these are in compliance with the IDEA Act and at par with the private sector at this point in time.

I will say, with every new project we come up with, we measure the ease with which customers or consumers or employers across the Nation are able to consume our services. So, are we shortening the amount of time taken for the business process to yield the results of mission outcomes? And those sort of success measures are in each and every one of our projects.

Mr. MAHANAND. So, this is Jay Mahanand from USAID.

So, like Mr. Ahluwalia, we also follow the IDEA's act, but we take it kind of, you know, a step forward. When I say we are 100 percent cloud enabled, we consider that as kind of the digital implementation of things that we do for the agency.

The ability for our staff overseas and locally to be able to get any of the services that they need should be—should be, you know, accessible to no matter where you are, and so we take that in terms of the insight in terms of our strategy and develop that—develop basically our architecture around that.

So it is, you know, something that we take very seriously given the fact that where we work in. We also have to look at our challenges of low-bandwidth, you know, areas in different parts of the world.

And so, when we look at digital technology, we also look at, you know, cloud services to be associated with that because, really, that's where the—you know, the rubber meets the road specifically when it comes to the digitization of, you know, services.

You know, we take something like digital forms, right? And so we've looked at DocuSign. And, you know, the ability for us to not necessarily be in the office to do that is something that, you know—that we would try to roll out for everything that we do.

So, it's just looking at what—you know, looking at the service themselves and seeing what we can actually digitize, or move it—again, move it to the cloud, where it is more accessible and then put the security around that.

Mr. COMER. So, what actions do you all take based on feedback from citizens and employees who use your agency's online tools?

Mr. MAHANAND. So, although it is—so, from—our primary interaction with users is—and the public is really through our main website, usaid.gov, and there is a feedback loop from that website

into the agency, and there is a team of folks that actually look at suggestions that comes in. And, if it's something that's viable, again, we act on it. But, if it is something that—you know, we modernize the site just to make sure that we are able to be everything in the IDEA's act, right, in terms of all five of those categories.

Mr. AHLUWALIA. We have a similar loop, Congressman. We take these things very seriously. And I'll give you an example. It was in my testimony earlier as well, the apprenticeship.gov website that we created.

We went to Job Corps centers. We went to jobs work centers, employment agencies across various states to figure out what is needed. We did a user-centric design study, and we continued that kind of a feedback loop to remain at par with the experiences these folks are getting with the private sector tools.

Mr. COMER. OK. Thank you, Mr. Chairman.

I yield back.

Mr. CONNOLLY. I thank the distinguished ranking member.

In closing, I want to reiterate some of the things we've heard here today.

We want to make sure there is full compliance with what's in the law, and nobody gets to sort of redefine that unilaterally.

Second, we do remain flexible with respect to the Scorecard, and we will be, as Mr. Hice suggested, remaining flexible and looking at categories to make sure we're capturing performance as accurately as we can.

And of course GAO has always been our partner in that regard, and we thank you, Mr. Walsh, and your colleagues for that continuing partnership.

And we hope that this kind of hearing—oversight hearing reinforces your ability to communicate with counterparts in respective Federal agencies that Congress means it. I can't think of another example on Capitol Hill for a single piece of existing legislation that has already had 11, going on 12, oversight hearings over five or six years on a very bipartisan basis, you know, to reinforce compliance and implementation. And so I hope that strengthens your hand as well.

And, you know, our goal is to try to make the Federal Government more efficient, to save money along the way. And we have saved a fair amount of money.

We want to followup on Mr. Biggs' question with you about supply chain vulnerability because I think—I think that might be the key to helping us better understand what happened and the how and why. The soft underbelly is the supply chain, and I think that's a pretty key takeaway from your testimony today, Mr. Walsh.

And, finally, I would ask—and, if you need a formal request, I think we'd do it, but I think all of us, on a bipartisan basis, would like to know, how did IT play a role in relief efforts—Federal relief efforts, and, for that matter, even state relief efforts related to Federal policy guidance in this pandemic?

You know, we look at the Small Business Administration and its E-Tran system, for example, that got overwhelmed. We look at the IRS, which had 60 different IT systems, some of which work well, some of which didn't. And, you know, it had to both remain the tax collector, audit entity, while also becoming a benefit delivery entity.

And that transition really challenged IRS in terms of its IT systems.

And then we also, of course, want to followup on legacy IT and the TMF and how we can best use that to leverage more—the acceleration of the retirement of legacy systems so that we're more cyber secure and we're saving taxpayers' money.

So, those are some things, I think, from today's hearing.

I want to thank my partner, Mr. Hice, and Mr. Comer for your presence here today as well.

One of the hallmarks of this—you know, we don't agree on a lot of things, but, when it comes to IT modernization, we've had bipartisan harmony coming out of this subcommittee. And, in fact, I'm very proud of the fact that the very first bill passed in the House in this Congress, on January 5, was a bill coming out of this subcommittee on a bipartisan basis, the FedRAMP bill, to codify the certification of private entities wanting to provide cloud services to the Federal Government.

And I thought that was a pretty strong statement about recognizing and elevating the importance and role of IT, which GAO first brought to everyone's attention in its high-risk report. So, we're continuing to try to take it seriously and push the system to betterment.

I thank my colleagues. This hearing is adjourned.

[Whereupon, at 10:27 a.m., the subcommittee was adjourned.]