FITARA 12.0

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

JULY 28, 2021

Serial No. 117–38

Printed for the use of the Committee on Oversight and Reform

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

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

RUSSELL ANELLO, *Staff Director*
WENDY GINSBERG, *Subcommittee on Government Operations Staff Director*
AMY STRATTON, *Deputy Chief 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

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

INDEX OF DOCUMENTS

The documents are available at: docs.house.gov.

FITARA 12.0

Wednesday, July 28, 2021

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

The subcommittee met, pursuant to notice, at 2:13 p.m., 2154 Rayburn House Office Building, Hon. Gerald Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Davis, Lynch, Khanna, Porter, Comer, Hice, Keller, Biggs, and LaTurner.

Also present: Representative Issa.

Mr. CONNOLLY. Welcome, everybody, to today's hybrid hearing. Pursuant to House rules, some members will appear in person. Others will appear remotely on Zoom.

Since some members or witnesses are appearing in person, let me first remind everyone that pursuant to the latest guidance from the House attending physician, all individuals attending this hearing in person are expected to wear a face mask in the hearing room, regardless of their vaccination status.

Members or witnesses may remove their masks when recognized by the chair to speak, and then kindly put the mask back on afterwards. Members who are not wearing a face mask risk not being recognized.

In addition, because we have a mix of vaccinated and unvaccinated people in the hearing room, we must maintain distancing to protect those who are not vaccinated.

Let me also state a few reminders for those members who are appearing in person. You will only see members and witnesses appearing remotely in the monitor in front of you when they are speaking in what is known as speaker view.

A timer is visible in the room directly in front of you. For members appearing remotely, I know you are all familiar with Zoom by now, but let me remind everyone of a few points.

First, you will be able to see each person speaking during the hearing, whether they are in person or remote. If you have Zoom set to speaker view or if you have questions about this, please contact committee staff immediately.

Second, we have a timer that should be visible on your screen when you are in the speaker view. Members who wish to pin the timer to their screen should contact committee staff for assistance.

Third, the House rules require we see you. So, please have your cameras turned on.

Fourth, members who are appearing remotely who are not recognized should remain muted so that we can minimize background noise and feedback and hear the person recognized to speak.

And fifth, I will recognize members verbally but members retain the right to seek recognition verbally. In regular order, members will be recognized in seniority for questions.

Last, if you want to be recognized outside of regular order, you may identify that in one of several ways. You can use the chat function to send a request, you may send an email to the majority staff, or you may unmute your mic to seek recognition.

Obviously, we don't want people talking over each other. So, my preference would be that members use the chat function or email our staff to facilitate formal recognition, and we will do the best we can to get back to you expeditiously.

We will begin the hearing in just a moment, and meanwhile, the chair would ask unanimous consent to recognize our colleague, the former chairman of the full committee, Darrell Issa, to be able to participate fully in this hearing.

Without objection, it is so ordered.

Committee will come to order. Without objection, the chair is authorized to declare a recess of the committee at any time. I now recognize myself for an opening statement.

For the past six years, this subcommittee has maintained a steady and bipartisan oversight of agency implementation of the Federal Information Technology Acquisition Reform Act in addition to other critical IT laws incorporated into the biannual FITARA scorecard.

The scorecard holds agencies accountable for improving their IT postures. In practice, the scorecard is a tool for Congress and the public to ensure better cybersecurity, reduce wasteful spending, and make government service to the Nation more effective.

Throughout this pandemic, we have come to realize how vital agile IT and strong IT governance are to the success of the Federal Government in meeting the needs of the people we all serve.

Today's hearing will discuss the results of the twelfth iteration of the FITARA scorecard. This hearing will also focus on how Congress and the administration can work together to improve services to this Nation.

We will examine how we can effectively modernize IT across the Federal Government, including making changes to administration guidance and adding new oversight metrics to the scorecard itself in order to hold agencies accountable for transforming how government does business.

Today, we will also hear for the first time from the new Federal CIO, Clare Martorana, about the administration's Federal IT priorities, including how it plans to administer the recent $1 billion technology modernization fund approved by Congress.

And, additionally, we will hear how she plans to prioritize projects to retire legacy Federal IT systems to accelerate agencies' transition to emerging technologies, improve Federal cybersecurity, and to implement actions from lessons learned from the pandemic.

The fact that Ms. Martorana is—am I pronouncing that right, Martorana—is here today is a clear indication of the Biden admin-

istration's commitment and recognition of the significance of FITARA and Federal IT investments themselves.

Since the December 2020 scorecard four agencies' FITARA scorecard grades increased, two decreased, and 18 remained unchanged. Nearly all agencies received a passing grade.

Unfortunately for some agencies and in some categories, progress has slowed. I hope to hear from our witnesses and OMB about transcending the hurdles to improved IT and to ensure efficient IT acquisition and management practices.

We must continue to strive for the dividends reaped from modernizing legacy IT systems, migrating to the cloud, and maintaining a strong and robust and protective cyber posture.

Despite some backsliding, the scorecard demonstrates continued improvements in many categories. Since the scorecard's inception in 2015, agencies have made substantial positive strides in improving their information technology practices.

For example, historically, agencies have reported that poor-performing projects are often broadly scoped and aim to deliver functionality several years after initiation. FITARA, however, requires agency CIOs to ensure that IT investments are adequately implementing incremental development practices and that functionality is timely.

Since 2015, the portion of agencies' IT projects implemented incrementally has risen from 58 percent to 78 percent. Among the FITARA scorecard categories with the greatest impact on taxpayer savings is the IT portfolio review process known as PortfolioStat.

Since 2015, the amount of money agencies have reportedly saved, including the costs they have avoided as a result of their PortfolioStat effort, has risen from $3.4 billion to $23.5 billion.

This increase includes $1.3 billion related to eliminating duplicative software licenses and about $7 billion in savings on data center consolidation. I might add, parenthetically, this committee will insist that the law be complied with in full.

The law circumscribes how data center consolidation is to occur and we will not suffer any delusion in the idea of data center consolidation or in the metric surrounding it.

We will insist the law be complied with and, if necessary, on a bipartisan basis I believe we are prepared to pass additional legislation for clarification if that is needed. Hopefully, it won't be.

I look forward to hearing from our witnesses on how they can continue to save taxpayer dollars while also ensuring agencies improve and fortify their IT infrastructures to better serve the public.

In addition to modernizing and acquiring the right technology, agencies must fill the skills gap in IT positions across the Federal Government, a big challenge.

Our Federal IT work force is rapidly aging into retirement. As of March 2021, 3.3 percent of the Federal Government's full time IT employees were under the age of 30—3.3 percent. Fifty-two-point-five percent were over the age of 50.

Federal agencies must focus on recruiting and hiring young IT professionals with the knowledge and skills needed to address the technology challenges of tomorrow.

At the very first FITARA hearing, former Department of Transportation CIO Richard McKinney stated, "IT is no longer just the business of the CIO. It is everybody's business."

Never has this been truer or clearer than in the wake of the coronavirus pandemic, where IT saved thousands of lives by enabling telework and keeping the government and the economy running.

We have seen firsthand how the agencies that continued to use outdated IT during the pandemic struggled to serve the very people who rely on them.

Some agencies remained mired in backlogs, including the National Archives and Records Administration, which failed to digitize critical veterans' records, and we are now paying a price for that.

The archives now reports a years-long backlog in providing veterans' access to records that qualify them for medical treatment, unemployment assistance, home loans, and student loans.

That is why I joined the ranking member, Mr. Hice, in urging the national archivist to apply for IT modernization funds so government can keep its commitments to our Nation's veterans.

Unfortunately, NARA is not the only Federal agency plagued by legacy IT systems. Congress and the administration must work together to prioritize IT modernization across the Federal Government.

With the Delta variant on the rise across the country and vaccinations flat lining, the stakes for effectively implementing FITARA are higher than ever.

When executed well, government IT modernization can ensure the efficient delivery of critical services. It can improve the government's knowledge and decision-making and save lives.

When executed poorly, it leads to outright failures in serving the American people when they need their government the most, and we have seen that too in the pandemic.

Simply put, the fate of the world's largest economy actually rises and falls in part with the ability of the government IT systems to deliver in an emergency.

The importance of Federal agencies' effective use of IT is too great to ignore, and this subcommittee won't waver in its continued oversight of agencies' IT acquisition and management.

And I might say, this is our twelfth scorecard hearing. I don't believe there is another committee in Congress that can match this record on a single piece of legislation in terms of oversight.

That is how committed we are and have been on a bipartisan basis throughout the years. And, of course, the co-author of FITARA, Mr. Issa, will be joining us a little bit later in the subcommittee hearing, and we are very pleased to have him back.

So, with that, the chair recognizes the distinguished ranking member, Mr. Hice from Georgia, for his opening statement.

Mr. HICE. Thank you, Mr. Chairman. I appreciate you holding this hearing.

And first of all, I do want to welcome Clare Martorana for joining us today and for your first time as the role of the Federal chief information officer. We welcome you here today.

Given your experience as an agency CIO, I really am interested to get your perspective on the FITARA scorecard and the IT dash-

board and, for that matter, actually, to help agencies' CIOs manage their portfolios and help OMB with its own government-wide oversight efforts or if these are just big reporting exercises. I look forward to hearing your perspective on all of that.

As the chairman said, this is the twelfth time that we have had a FITARA scorecard. I know it has changed over time. But to me, the overriding question is and always will be are we spending Federal IT dollars well.

I mean, at the end of the day, that is the issue. And, you know, are projects coming in on time? Are they on budget? Do they do what they are supposed to do? Why or why not?

I mean, these are just basic questions that we need to face and that we need answers for, and that we need to keep a pulse on as we go through all of this.

These are important questions, and the answers to these questions shine the light on pretty much everything else, whether it is procurement, work force, organizational structure, culture, and on and on. So, the score card has evolved in the past.

Frankly, I think it is time that we take a fresh look at the whole FITARA process through the lens that I have just described, with any reported metrics reflecting measurable legislation or executive branch policies. We have got to be objective and quantifiable, and it needs to be reported in a matter that is comparable agency to agency.

So, I get it that all of that is probably easier said than done. I mean, I know that. But nothing around this place is easy. But I would like to take a good look at these type of things, frankly, before we move on to FITARA 13 and 14.

I also think the subcommittee needs to take a good look at a few other issues, Mr. Chairman, and I would put this out there. What is the state of IT modernization, generally speaking? I know Congress passed the MGT Act and now there is billion of dollars, really, in technology modernization. Those funds are to be spread around.

But what is its impact? What are we really getting in relation to modernization? Is it happening? Is it having the impact that it is going to point toward the kinds of modernization experiences that you have described in your testimony, Ms. Martorana?

Second, are our systems safe? This is an issue that has come up time and again in hearings. As much as any system can be safe, are our systems safe?

In its testimony, the GAO's top concern revolve around cyber issues. It is an issue we have got to deal with, and I believe the scorecard needs to hone in on those types of questions.

Given the critical nature of the topic, is it enough just to have it to be a subcomponent of the broader scorecard? Or is it time to figure out a way to shine the spotlight on this area without tipping off the bad guys of our vulnerabilities? I think we have got to address this.

And then, finally, how well are the American people being served? I think the scorecard needs to reflect this. At the end of the day, the Federal Government is here to serve the American people, and we need to know how effective we are doing in that.

How easy is it to access government services and benefits through digital means? In the private sector, you don't survive for long if you don't excel in this area, and I believe we need to take a look at it on the Federal perspective as well.

And, Ms. Martorana, again, in your testimony we share the view that you said, quote, "The Federal Government is fundamentally in the service business." I totally agree with you on that. In fact, I couldn't agree more.

So, all of the items that I have mentioned here are important. But I would like to specifically ask my colleague from Virginia, Chairman Connolly, if we could look at some of these issues, going forward.

I think these are worthy not only of attention, but of fine tuning the scorecard as a whole. I will put that out there. I am not finished but——

Mr. CONNOLLY. I will respond to my colleague, of course, and, in fact, I definitely see the FITARA scorecard as always a work in progress.

Mr. HICE. Right.

Mr. CONNOLLY. And the only caution is, as you can see from the grades in front of us, we have not yet succeeded in full implementation.

So, we don't want to lose our sight of that. But we also always want to be capturing other dynamics as we learn and as we see performance in the Federal Government.

So, I couldn't agree with you more.

Mr. HICE. I thank you, Chairman.

Mr. CONNOLLY. And, absolutely, we will work with you.

Mr. HICE. Thank you, Mr. Chairman.

And the last point I will make is this. I have made clear the focus of the administration. They should be having Federal employees return to their offices. But I am concerned that the emphasis instead appears to be on institutionalizing expanded telework.

So, I am glad that we are joined by the CIO of the Social Security Administration today as well. So, this is one of the agencies facing the greatest challenge in providing the American people with services that they need, and if SSA is not going to reopen more rapidly then I will be interested to learn how improved IT can help improve citizens' experience.

So in closing, again, I want to thank our witnesses for being here. I am eager to hear the insight and the suggestions as we move on to FITARA 13 and 14 and beyond. I look forward to hearing our discussion today.

And with that, Mr. Chairman, I yield back. Thank you.

Mr. CONNOLLY. I thank the ranking member, and I thank him for his cooperation in this and other endeavors.

I see we have been joined by the ranking member of the full committee. Does he wish to make any statement?

OK. Welcome, Mr. Comer. Glad to have you.

With that, let me introduce our witnesses. We have four witnesses today, and I am going to swear them in. But, first, let me introduce them.

Our first witness is Clare Martorana, who is the Federal Chief Information Officer, finally, at the Office of Management and Budget. We are so glad to have you today.

Then we are going to hear from Keith Bluestein, Chief Information Officer at the Small Business Administration.

Third, we will hear from Sean Brune, Chief Information Officer of the Social Security Administration.

And finally, we will hear from our long partner, Carol Harris, Director of Information Technology and Cybersecurity at the GAO, the Government Accountability Office, which actually helped design and continues to help us update and modify the scorecard.

If all of our witnesses could stand and raise their right hand to be sworn in, which is the custom of this committee and subcommittee.

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

[Witnesses are sworn.]

Mr. BLUESTEIN. I do.

Mr. CONNOLLY. Mr. Brune?

Mr. BRUNE. Yes.

Mr. CONNOLLY. Yes. OK. Let the record show all four of our witnesses have answered in the affirmative. You may be seated. Thank you.

With that, Ms. Martorana, you are recognized for your opening statement. We will ask all of our witnesses, if you could, your full statement will be entered into the record as written. We would ask you to try to summarize your testimony in a five-minute opening statement.

Ms. Martorana?

STATEMENT OF CLARE MARTORANA, FEDERAL CHIEF INFORMATION OFFICER, OFFICE OF MANAGEMENT AND BUDGET

Ms. MARTORANA. Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you for the invitation to testify about the twelfth FITARA scorecard.

Technology enables mission delivery. It is FITARA that gives every CIO a seat at the table to make the best IT decisions to deliver for our citizens, and it is enterprise collaboration that will be key to making it all happen.

I would like to thank the committee for your leadership promoting modernization. I believe we must take on this challenge together to secure Federal IT and deliver transformational services to the American people.

I would also like to acknowledge Sean, Keith, and fellow—my fellow CIOs and the entire IT work force across our government for their hard work to achieve the grades on this scorecard.

Imagine the day when a citizen can use their mobile phone to sign in and see everything that they have in flight with our government—a small business loan application, the status of their tax refund.

Imagine the process is easy, understandable, convenient, secure, and fast, just like the experiences we have with online banking and food delivery.

With the amount of information we collect across the Federal Government and the enormous investment of taxpayer dollars in Federal IT, this vision is not only possible, it is an expectation in the 21st century.

For over 20 years in the private sector and the past five years in government, I have used innovative technology and human-centered design to improve people's lives. As Federal CIO, I will use my expertise to scale these successes across the Federal enterprise.

Federal employees are counting on us and, more importantly, your constituents, the American people, are not only counting on us, they are asking us to move faster.

We can get there by focusing on three priorities that I address, the long term goals and urgent circumstances we find ourselves in today.

First, cybersecurity is our immediate priority in Federal IT. Cybersecurity is a national priority. I am committed to ensuring every agency is ready for today's threats.

The cyber executive order puts us on a good path to faster incident response and stronger protective measures. By working rapidly and seamlessly, we can achieve results and we must. Our adversaries are on the move and they are aggressive.

Second, I am committed to modernizing Federal IT. The $1 billion appropriation to the Technology Modernization Fund, or TMF, is an important start to improving the government's IT systems.

But it is just a down payment on the multi-year technology modernization projects Federal agencies have identified. The TMF board has received 108 proposals in our accelerated model, totaling $2.1 billion since the rollout of the funding provided by the American Rescue Plan.

And third, we must focus on service delivery to the American public. It is not our citizens' job to figure out how to navigate across a department or agency silos to gather the services they deserve.

That is our job. By transitioning agencies to a product mindset organized around users, we can deliver modern efficient tools and technology, reduce administrative burden, and spend more time on high-value services to the public.

These challenges have highlighted our need to rethink our approach to Federal IT. We must identify new ways of working across government, such as developing playbooks that build on what we know already works, collaborate more frequently with key stakeholders to focus oversight on the work being done today, and rethinking how we are working in the office of the Federal CIO, such as pairing technologists with our policy experts at the beginning of the process to develop innovative technology solutions within our laws, rules, and regulations.

Finally, we must optimize for results, not optics. We need to show, not tell, and deliver on our mission. As we begin this new chapter of Federal IT modernization, we are building on a strong foundation.

I am excited to enable the government's diverse missions as Federal CIO, and I look forward to partnering with Congress.

Thank you for the opportunity to testify today and I am happy to take your questions.

Mr. CONNOLLY. Wow. That is a pro. You had 11 seconds left. I am impressed. Great start, and we look forward to working with you as well.

Mr. Bluestein—is it pronounced Bluestein or Bluestein?

Mr. BLUESTEIN. Bluestein.

Mr. CONNOLLY. Mr. Bluestein. Excuse me.

Welcome.

STATEMENT OF KEITH A. BLUESTEIN, CHIEF INFORMATION OFFICER, SMALL BUSINESS ADMINISTRATION

Mr. BLUESTEIN. Good afternoon, sir.

Chairman Connolly, Ranking Member Hice, subcommittee members, thank you for the opportunity to discuss the Small Business Administration's implementation of FITARA.

Much has changed since the last time we talked to you about FITARA in 2017. To the great benefit of SBA and America's small businesses, FITARA has provided the critical structure in tools for SBA to optimize, modernize, and innovate while investing in the IT work force of tomorrow.

I would also like to add some other benefits that SBA has enjoyed, courtesy of the Modernizing Government Technology Act of 2017, or the MGT Act.

This modernization foundation was vital in enabling exponential scaling of SBA's operations to deliver the Nation's largest ever economic recovery initiative in a very short period of time.

Just to recall the scale, by October 2020, SBA's disaster program approved and disbursed more than three times as many funds for the COVID–19 EIDL program as we had for all disasters combined in the agency's 67-year history.

On the capital-access side, SBA issued more loans in 14 days than they had in 14 years. The scaling challenge was daunting, and while there were some hiccups along the way, SBA's IT infrastructure proved to be resilient, scalable, and adaptable to the changed business requirements, such as transitioning to the maximum telework model.

When I rejoined SBA in June 2020 as the CIO, SBA had already adapted to the changed conditions due to the COVID–19 global pandemic.

The flagship economic recovery programs, EIDL and PPP, were already in high gear, and the SBA work force was rapidly surging up after smoothly transitioning to remote work.

An accelerated deployment of online collaboration tools and training had helped the SBA staff to continue to be productive and not miss a beat while maintaining a robust security posture.

FITARA had solidified the coordination and collaboration between the CIO and the chief human capital officer and the chief procurement officer. These two relationships and the supporting infrastructure that resulted were the key underpinning foundation that enabled the SBA surge for the pandemic response.

We tend to focus on technology with CIO-related activities. But FITARA took a much broader approach to how the CIO becomes a valued mission partner in the agency. The pandemic relief and, more specifically, the CARES Act, brought into clear relief how important these relationships are.

Had they not existed prior to the passage of the CARES Act, there is likely no way SBA could have responded with the speed that we did. SBA surged from approximately 5,000 employees to over 18,000 in only a couple of months.

Hiring on that scale was unheard of prior to the pandemic, but the personnel relationships that had developed and cultivated were crucial to this rapid expansion.

Similarly, the need for immediate increase in technical support for the agency's systems and employees called for acquiring huge volumes of laptops for remote work servers, cloud services, software licenses, and contracted support teams.

This was a testament to the great team that procurement organization had in place. The ability to surge to the level that was needed to support all the CARES Act activity was enabled by the tight nexus that had been formed with the CIO and CFO through FITARA.

Looking back now, it is hard to imagine how SBA would have been able to support the CARES Act activities successfully without the prior work that had been prescribed by FITARA.

I would like to highlight other legislation as well. One of the many IT modernization tools you provided government agency is the IT Working Capital Fund, provided for under the MGT Act.

We have taken full advantage of this capability that afforded great flexibilities to CIOs, especially in agencies like ours where we deal primarily with one-year appropriations.

The Working Capital Fund allows SBA to have a long-term vision for modernization with a managed resource pool to ensure that that vision is realized.

This tool helped bolster FITARA by strengthening the collaborative bond the CIO has with the CFO to execute the agency's mission. MGT was a welcome adjunct to FITARA and has allowed SBA to better plan and resource expenditures on a multi-year horizon.

A sampling of some of these projects included modernizing SBA's infrastructure, unifying and enhancing the customer experience, updating support for all small business certification programs, and improving systems that manage entrepreneurial development, to name just a few.

I want to circle back on FITARA, though, to highlight that none of the success comes without the critical support of the administrator and our immediate leadership team.

FITARA is very clear about the importance of the relationship between the department or agency head and the CIO. That importance cannot be overstated, but I don't know that a solid line in an organization chart always captures the level of support that the CIO receives. I understand that scoring and the FITARA scorecard reflects less favorably for SBA and other CIOs without a solid-line relationship.

But I can tell you, personally, that I have unmitigated and total support from both the former and current administrators. While that is a feature envisioned in FITARA, I know this may not always manifest itself the same way in every agency.

I am fortunate. SBA's top leadership always ensures the CIO has direct access and has a seat at the table and their voice is heard.

The visibility and inclusion helps to ensure that the decisions do not get made in a vacuum or in a siloed fashion, and that such resources are allocated such that the maximum benefit is realized across the agency.

In closing, it bears repeating that the extensive improvement in SBA operations is a direct result of the implementation of FITARA.

Thank you for the opportunity to share SBA's progress on FITARA implementation, and we look forward to answering any questions you may have.

Mr. CONNOLLY. Thank you, Mr. Bluestein.

Mr. Brune, you are recognized for your five-minute summary testimony.

STATEMENT OF SEAN BRUNE, CHIEF INFORMATION OFFICER, SOCIAL SECURITY ADMINISTRATION

Mr. BRUNE. Thank you.

Chairman Connolly, Ranking Member Hice, and members of the subcommittee, I am Sean Brune, Social Security Administration's Deputy Commissioner for Systems and Chief Information Officer.

Thank you for inviting me to discuss the role of information technology and the Federal Information Technology Acquisition Reform Act, or FITARA, in delivering Social Security services to the public.

As a former regional commissioner, I know how vital modern technology is to carrying out our mission. I also appreciate the importance of managing and monitoring information technology investments, a key tenet of FITARA.

Effective use of technology is mission essential. Our employees use technology to collect and store information, pay benefits, and identify and prevent fraud and improper payments.

We have known for years that we must modernize our IT and we are well on our way, phasing out legacy systems and aligning our IT infrastructure with FITARA requirements. We began modernizing our IT framework by building a virtual private network, or VPN, nearly two decades ago.

Since then, we have continued these efforts. In 2015, we began replacing desktop computers with laptops. In 2017, we released an initial comprehensive five-year IT modernization plan, and in 2019, we converted to cell phones for improved mobility and established the role of the Chief Business Officer to partner with the CIO and ensure our IT investments are customer focused.

Our initial 2017 IT modernization plan focused on replacing aging systems and improving service through technology. In 2020, we updated this plan to accelerate delivery of modern software and expand self-service options.

The 2020 update is our current roadmap, and we will continue to update it and prioritize IT initiatives as needed to align with the agency's strategic goals.

The pandemic underscored the importance of IT to our mission and highlighted the success of our modernization efforts.

Last March, when we shifted to telework to keep everyone safe, our secure VPN, laptops and cell phones helped us transition over 90 percent of Social Security employees and thousands of state employees who make medical determinations to telework within a few weeks.

Technology has allowed us to continue to serve the public through online and telephone services, while we limited in-person service to critical situations.

The pandemic also emphasized the need to further expand electronic self-service options for the public and to restructure outdated work processes.

To meet our customers' needs, we quickly implemented new electronic signature options, modern processes for submitting forms online, and increased their use of video to conduct disability hearings.

This year, we began rolling out a modern unified communications platform to improve customer service when people call us. We are also revamping our public-facing website, *socialsecurity.gov*, to streamline content and redesign the homepage. We plan to fully implement the new website next year.

Technology supports improving public service. FITARA and this committee's scorecard help us assess our progress in managing our IT infrastructure and provide guideposts for improvement.

In accordance with FITARA, we make informed funding decisions on IT investments by leveraging some commercial off-the-shelf products and executing incremental product deployment.

As a result, we have maximized resources, expanded digital services on our online channel, My Social Security, and ensured the security and stability of these new service options.

Moving forward, we will offer more streamlined and automated self-service options and enhance in-office service for people who need them while maintaining a robust cybersecurity program.

We appreciate President Biden's Fiscal Year 2022 discretionary request of $14.2 billion, which will help us continue to build the secure, efficient, customer-centric IT infrastructure of tomorrow.

In closing, I want to thank our Social Security employees for their resilience and dedication to our mission during this challenging time.

I appreciate the opportunity to be here today to update you on SSA's progress and I look forward to answering any questions you may have.

Mr. CONNOLLY. Thank you, Mr. Brune. Right on time. And we join you in thanking all of our dedicated public servants in all of our Federal agencies who have continued to function and serve the American public during this unprecedented pandemic. Thank you.

Ms. Harris, welcome back. What do we need to know?

Ms. HARRIS. Thank you.

Mr. CONNOLLY. You are recognized.

STATEMENT OF CAROL C. HARRIS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. HARRIS. Chairman Connolly, Ranking Member Hice, and members of the subcommittee, I want to thank you and your excellent staff for your continued oversight of Federal IT management and cybersecurity with this twelfth set of grades.

Your scorecard continues to serve as a key barometer for measuring FITARA implementation as well as other essential IT reform initiatives.

Since the December 2020 scorecard, progress made by the agencies to implement FITARA has slowed a bit, with 18 agencies' overall grades unchanged, two with decreases, and only four with increased grades.

Most agencies receiving a pass—most agencies received a passing C or higher grade, with DOJ receiving the only D. GSA was the only agency to receive an A for this iteration. I will now share some key highlights from this twelfth scorecard.

First, cybersecurity continues to be an area of struggle for the agencies. One-third of them have a D or F and another third are getting by with a C.

This is also consistent with our body of work in Federal cybersecurity. We have reported on the agencies' need to address information security program weaknesses, including establishing an enterprise-wide cyber risk management program.

For example, in July 2019, we found that while the 23 civilian agencies almost always designated a risk executive, they had not fully incorporated other key risk management practices, such as setting up a process for assessing agency-wide cybersecurity risks.

Having mature cyber risk management programs would help agencies improve in the areas that the IGs are looking at and, in turn, increase their cyber grades on the scorecard.

As another example, in December 2020, we found that few civilian agencies had implemented foundational practices to mitigate global IT supply chain risks.

In the wake of the SolarWinds incident, which involved a software supply chain compromise, the need for robust and comprehensive supply chain risk management program is essential.

We have, roughly, 950 open recommendations to the agencies in OMB, covering a range of cyber-related issues, and actions are needed to—are needed on these to help improve our Nation's cybersecurity posture.

Now to my second point. About half of the agencies have an MGT Working Capital Fund or have plans to set one up by 2022. These funding vehicles, along with the Technology Modernization Fund, are intended to help agencies tackle their legacy IT problem.

At least 60 percent of the Federal Government's IT spend each year goes toward maintaining aging systems. Only 13 percent is spent on modernization projects.

Establishing these funds are critical so that savings from data center optimization and PortfolioStat efforts can be reinvested in agency IT modernization priorities, and the recent gains by the agencies in this area would not have been possible without your persistent leadership. So, thank you very much there.

I will now turn my comments to SBA and SSA. These agencies, collectively, plan to spend $2.1 billion on IT this year. SBA spends about 80 percent of its IT budget maintaining legacy systems while SSA's is about 60 percent.

SBA has an overall C+ grade, which is a slight decrease from its solid B+ performance in years past. SSA has made some noteworthy progress from its D grade on the first scorecard back in 2015 to a B+ today.

Some positive areas to highlight for both, they have achieved their data center closure goals as well as completed most of their optimization and savings goals for the fiscal year.

The SBA and SSA CIOs also report directly to the heads of their agencies. For SBA, progress in the area of IT portfolio review continues to be lacking. Its savings ratio was ranked 21st among the agencies with $14 million in reported savings and cost avoidances since 2012. For SSA, the level of transparency in its evaluation of major IT investments could be improved.

The agency spent $177 million on major IT in Fiscal Year 2021 and did not rate any of those investments as red, leaving SSA ranked 20th among the agencies in risk transparency.

Mr. Chairman, that concludes my comments on the overall scorecard and the results for these two agencies, and I look forward to your questions.

Mr. CONNOLLY. Thank you very much.

I just, editorially, want to remind everyone, the word Mr. Issa and I wrote into the law is consolidation, not optimization, and it is a legal requirement to consolidate data centers.

When we began that effort, Mr. Vivek Kundra, then your—well, I guess he was CTO. But he estimated, I want to say, and this is 2009, that the Federal Government overall had something like 1,800 data centers and he proposed we cut them in half.

And in our law, we basically said we will cut that in half again. You know, get them down to 450 or something like that.

Well, when we had our first hearing on how are we doing, we not only didn't make any progress in consolidation, the only progress we made was in identifying the fact that we had a lot more data centers than we thought, and I want—I want to say it was something ridiculous like 12,000 or something like that, the first iteration. So, we got really good at identifying, well, there is one, there is another one.

But our point was it is inefficient and there are savings to be had and we have to do that. And so you inherit this slight contretemps from OMB that has sought, from our point of view, to dilute what the law stipulates. And it is not just that we are being critical.

We, honestly, think it is a worthy goal to urge people to consolidate and move to the cloud. So, we want to work with you. And that is just an editorial comment, not a question, but we can get into that later.

The chair now recognizes the distinguished Congresswoman from the District of Columbia, our friend, Ms. Norton for her five minutes of questions.

Ms. Norton?

Ms. NORTON. I thank my good friend and regional partner, Mr. Connolly, for this hearing.

And I want to—I want to ask questions about how outdated our legacy systems are and what we can do to modernize them.

We saw examples of that during the pandemic, which is why I want to raise this issue, because they prevented continuity of agency operations in some critical cases.

Let me start with Ms. Martorana, because I appreciate your remarks on the importance of modernizing Federal IT.

Now, I want to recognize the complexity of that process, which, unfortunately, gets oversimplified by thinking about certain systems as either legacy or modern.

So, Ms. Martorana, can you talk about how to look at the modernization process and the prioritization of Federal IT modernization efforts?

Ms. MARTORANA. Thank you for that question. I appreciate it.

I think you hit on a key point, which is modernization is a continuous process. Every system is at a different stage of needing modernization, and we have a complex set of environmental challenges with both end-of-life systems that we have to modernize across the Federal enterprise, and also innovative and evolving technology that we would like to continue to support, like the CloudSmart Initiative and continuing to move our Federal work force and our IT posture into the safest, most secure disposition that we possibly can.

So, I think that the opportunity to utilize programs like TMF are really a significant movement forward in our ability to actually deal with the IT modernization challenges in front of the government.

Ms. NORTON. Thank you.

Let me go to Mr. Brune because of how far Social Security may be. In 2017, Social Security spoke of a five-year IT modernization plan. I would like to know how this plan has helped Social Security prioritize the retirement of legacy systems.

Mr. BRUNE. Thank you, Congresswoman, for the question.

We are in the tail end of the fourth year of our five-year modernization plan. That plan has focused on addressing older legacy core mission systems, the systems that are used to pay retirement insurance benefits, disability insurance benefits, and to issue Social Security number cards.

We are on track, on schedule, and on budget with our plan. We appreciate that Congress has appropriated dedicated appropriations to support our multi-year plan, which has allowed us to plan and execute development and procurement across fiscal years.

Some of the results of our plan are increased use of our online channel. We have over 60 million persons across the Nation who have a My Social Security account, a secure portal where they can see, as the Federal CIO said in her opening statement, what the status of their Social Security benefits is.

If they are still working and planning for future retirement, they can get an online estimate of their personalized retirement at any point in time. If they filed a claim they can check on their—on the website or on their phone what the status of their claim is.

We have also improved our use of the online channel and the phone channel for handling work during the pandemic by allowing scheduled appointments and by increasing our use of video service.

Ms. NORTON. I see my time has expired. Thank you, Mr. Chairman.

Mr. CONNOLLY. Thank you, Ms. Norton.

And I would just add, Mr. Brune, to your list of impressive achievements I have been impressed with your ability to flag fraud or attempted fraud, which I think is really a protection for the American consumer and beneficiary of Social Security.

I don't know quite how you do it, but I was almost a victim myself and it was Social Security that caught it and had a solution for it.

So, I was personally really impressed. If you are doing that across the board that is a great use of technology to protect the American people.

Mr. Hice is recognized for his five minutes of questions.

Mr. HICE. Thank you very much, Mr. Chairman.

Ms. Harris, let me begin with you. You brought up in your testimony that some of the top items, in fact, really the top item, I believe, was your wording, that GAO lists for action deals with cybersecurity, and I certainly agree with you on that.

But looking at the current scorecard that we have makes me just wonder a couple things. First of all, is cyber, in your opinion, weighed heavily enough in the FITARA scorecard?

Ms. HARRIS. Well, I think that is certainly—you know, I am always happy to have my team work with you and your staff to make sure that the purpose of the scorecard is meeting your oversight needs, first and foremost.

When it comes to cybersecurity, I think that there—it is multi-dimensional and, certainly, with the FISMA grade itself as it—as it is shown on the scorecard, I mean, that is measuring one dimension of cybersecurity, but there are certainly others.

So, again, you know, when we take a look at the scorecard, it is—it is really ensuring that it is fulfilling the purposes of your committee and as far as oversight is concerned.

So, we are happy to take a look and evolve that at—you know, at your direction.

Mr. HICE. Well, based on that, then would you be in favor or do you think it would be wise for us as a subcommittee to consider cybersecurity as an independent issue? Should there be a scorecard that focuses specifically on cyber?

Ms. HARRIS. We would be happy to entertain that and see what can be done. I think one of the challenges that we have as far as either expanding the current FITARA scorecard to include additional areas of cybersecurity or having a stand-alone cyber scorecard is the availability of public data because, certainly, we don't want to put agencies at greater risk in identifying those and pointing out those vulnerabilities publicly.

So, I think that is the greatest challenge that we face.

Mr. HICE. Yes, no doubt. That is—that is a challenge, and we have got to be very careful with that. At the same time to have appropriate oversight as it relates to cyber issues, we need some sort of, within this context of this hearing, a scorecard to determine how are we doing on the cyber issues.

So, you would be willing to work with us on trying to figure out some sort of plan? And when I say us, it would be me and the chairman as well. I mean, let us try to deal with this.

Let me ask you this, and this is a question I have had for a long time and I think you are the one to ask.

In previous FITARA hearings, it was stated that over $22 billion have been saved, attributed directly to FITARA. I can't figure out where that figure comes from. What is the—what is the metric? How is that figure determined?

Ms. HARRIS. It is agency-reported data, and that is coming out of data center consolidation as well as PortfolioStat efforts.

And we have not taken a systematic look at the savings that are being reported by the agencies in terms of how they are reinvesting that—well, first of all, collecting and reporting the total savings that they are getting from these initiatives as well as how they are reinvesting it.

So, but I can tell you, though, that what you just cited right there comes from data center consolidation and PortfolioStat initiatives.

Mr. HICE. But we are not looking into it to see if it is accurate. Is that what I am hearing you say?

Ms. HARRIS. Well, we have not, but we are, certainly, happy to take a deeper look into that. I think that that would be a very insightful review that we would be happy to do for you.

Mr. HICE. Yes, I think it would be very insightful, too, and, you know, obviously, we don't have the same—I don't have access to the same information you have in looking at all this.

But I see those numbers thrown out there and I am just curious. I mean, that is a great number, if it is accurate, but I want to know where does this come from and what is the accuracy of it, and it sounds like you really have the same kind of questions because you have not been able to dig deep to see just—OK.

All right. Well, with that, Mr. Chairman, I will—I will yield back.

Mr. CONNOLLY. I thank the chair—I thank the ranking member and I would just caution, let us verify that number right after our elections.

[Laughter.]

Mr. CONNOLLY. All right. The incredible gentleman from Massachusetts, who represents my family back home in Boston, Mr. Lynch.

Welcome, and you are recognized for your questioning.

Mr. LYNCH. Well, thank you very much, Mr. Chairman, and thank you for this very, very important hearing.

You know, I would like to just offer this out for the witnesses. You know, there is such a gap in IT talent, generally, but especially in the Federal Government, because we—we have got this turnover.

We all have bright young people that come to work for us and when they gain a certain amount of ability and technical skill, they move on because of higher salaries that we cannot offer them.

But, generally, in the IT work force across the Federal Government, there is a real skills gap. I think right now we have got about—a little more than three percent of the IT workers in the Federal Government are under 30 years of age and half of the IT work force is over 50. So, we got about—we got to think about playing the long game here.

You know, China does this. They think in terms of decades, and one of the—one of the solutions, I think, is really to have Federal resources. You know, encourage and build incentives for young people to get into STEM-related professions.

So, I found that in Boston I founded a charter school based on STEM. Basically, we did—we took the curriculum that the regular

public schools has in Boston and then we tripled the amount of math and science that these kids are exposed to over their—over their, you know, grammar school and high school lives.

So, we are having great results, and that is without incentives, right. That is just offering that school, and it is a lottery. We have probably one of the most diverse populations in that school—you know, kids of every race, ethnicity, you know. It is—it is a model to behold.

But we need to do more on a bigger scale, and I am just wondering, do we have any programs that, let us say, offer these young people help with their student loans or are there any programs where we actually support schools like my charter school that focus on, you know, STEM education so that we create this work force of the future?

There is such a huge gap right now. We can't close it in the short term, not under the existing circumstances. But over time, you know, we can—we can close this gap, but only if we take deliberate action and we stick to it.

And I am just wondering, on that skills gap issue if any of our witnesses have any recommendations or any examples that provide best practices on how to—how to fill that gap and how to—how to put the right people in the right positions to move the country forward and to protect us.

Mr. CONNOLLY. Ms. Martorana, I think you are best positioned to begin to answer that question.

Ms. MARTORANA. Thank you very much for the question.

The administration is focused on building a world-class team of professionals with skills in these critical technology areas. We have an enormous resource in our Federal Government with our Federal employees.

I really encourage us to continue to look at re-skilling and up-skilling opportunities in our government with our own Federal work force.

In addition to that, there are numerous programs that are going on across the Federal Government: the United States Digital Service, 18F, the Civic Fellows Program. So, there is a lot of effort in this area and I think that we have a great opportunity because people have a desire to serve our country, and there are many different channels that we can plug into to make that opportunity available.

I am a great example of someone who came to do a tour of service and wound up being so inspired by the mission that I felt the need to stay and continue to work in this environment.

So, I think that there are opportunities. I know the administration is focused on making sure that our work force looks like our country and that we have opportunities to recruit cyber talent, IT talent, and other subject matter experts across our government.

Mr. LYNCH. I appreciate that, Ms. Martorana. But it is a different—well, first of all, it is a very—it is a smaller pool of people when you just look at our Federal employees, and I personally know some Federal employees that are still walking around with flip phones.

So, what we are trying to do is increase that pool of talent. It will not only help the Federal Government, it will help private in-

dustry, and first of all, it will help those kids because, you know, we have found that regardless of background, if you have a program of total immersion with these young people, and you have a 12-year runway of their education, you can really make a big impact on increasing the pool of talent and the quality of that talent, going forward.

So, if we are—you know, if we are training somebody who is 50 years old, you know, there is a limited horizon for that worker between investing, training, and then they are off into retirement.

So, what I am suggesting is to lengthen out that runway and populate it with a much larger population that we could train. But maybe that is something I need to work on in terms of, you know, a scholarship program or something like that that would be available to these grammar schools.

It does fit very neatly with the president's initiative to offer universal Pre-K where we get kids in at that early age and we provide them with, you know, the rudimentary beginnings of an education in STEM.

So, with that, Mr. Chairman, I thank you for your kindness. I thank you for all the great work that you do. I want to thank our witnesses. Very important issue.

And I yield back. Thank you.

Mr. CONNOLLY. Thank you, Mr. Lynch, and you really raise a good point about the need to recruit and retain the work force of the next generation, and I would love to work with you, Mr. Lynch.

I have a bill I am developing on using the Federal—a Federal internship program to populate the vacancies we are projecting for the future.

We do a lousy job of Federal interns compared to the private sector, and so it is something ripe for improvement that could actually be a huge part of the solution, including in the IT sector itself.

So, I look forward to working with you, Mr. Lynch, on that.

Mr. LYNCH. Happy to do that. Thank you, Mr. Chairman.

Mr. CONNOLLY. Thank you, Mr. Lynch.

Mr. Keller is recognized for his five minutes.

Mr. KELLER. Thank you, Chairman Connolly and Ranking Member Hice, for having this hearing. Also, thank you to our witnesses for participating and joining us this afternoon.

The FITARA scorecard remains a valuable tool in assessing the modernization of the Federal Government's IT system and cybersecurity infrastructure. Strengthening our Nation's IT infrastructure and cyber grid is a goal we can all work toward.

The Federal Government spends, roughly, $100 billion on cybersecurity and IT investments annually, yet we still face challenges securing some of our Nation's most sensitive IT systems.

These challenges have been highlighted by the recent events such as the Colonial Pipeline and SolarWind's cyber attacks. Congress and the administration must now look at cost-effective strategies to improve our Nation's IT systems and cyber readiness.

Ms. Martorana, I have concerns regarding the cost of implementing technological changes. In December 2019, Congress appropriated about $125 million to the Technology Modernization Fund.

However, agencies encountered financial problems with monitoring the fund. As of June 2021, approximately $89 million of the

fund has been awarded to 11 projects across seven Federal agencies. Not even 10 percent of the money allocated for these—in this fund.

What tools can Congress provide to OMB to improve cost estimating practices?

Ms. MARTORANA. Thank you very much for that question.

It is—OMB is committed to full transparency in Federal IT spending and performance data. So, we would welcome feedback and continued collaboration on making sure that we are completely transparent on those numbers.

With relation to the Technology Modernization Fund, I can't speak very in detail about what happened prior to me joining. But I can tell you a little bit about how we are utilizing the Technology Modernization Fund since we have been appropriated the additional $1 billion under the American Rescue Plan.

We have—as I said in my opening statement, we have 108 projects that have come in from 43 different agencies, and I think it really represents the market demand for flexible IT modernization funding and our ability to work collaboratively to continue on the IT modernization journey that most agencies have a pretty significant backlog in their own portfolio for these projects.

Mr. KELLER. You had mentioned that you couldn't speak before you came into the agency. Are some of the same people in the agency today that were in when we had appropriated the money before with this new money that you referenced in the—in the American Rescue Plan?

Ms. MARTORANA. I am sure that there are some OMB employees that are—have been in tenure during the length of TMF being stood up.

But I can really tell you since I have joined there is a real commitment not only to the TMF and the IT Modernization Fund, but we are having very active conversations with all of the staff at OMB about agencies' needs, focused on cybersecurity as a primary, but IT modernization goes hand in hand with cybersecurity.

Mr. KELLER. So, you have taken proactive steps to make sure the same thing doesn't happen with this money as happened with the previous money that you can't tell us about? I mean, that you can't reference since you weren't there?

Ms. MARTORANA. Yes, we are working kind of on a two-pronged strategy. One is when we identified the payment flexibility for TMF under the American Rescue Plan, we asked—put out a call to agencies saying, come and tell us in four category areas where you need the most investment, and that was high-value assets that need to be modernized, cybersecurity, public-facing digital services that were identified through the COVID pandemic, and shared services where multiple agencies could benefit.

And so under that framework agencies came to us with this 108 project proposals and they are still coming on a rolling basis. We also, as a board, want to take a top-down look as well to see where we can have the greatest impact across the greatest number of agencies.

So, take an area like cybersecurity. We don't start from a blank piece of paper, right. Any of the—my fellow CIOs would probably attest to the same. We are all trying to solve the same problems

whether we have legacy IT, end-of-life systems, or systems that are a little bit more modern but could benefit from innovation that is going on in the private sector.

So, we are looking from a top-down perspective as well as really trying to source from agencies' need directly.

Mr. KELLER. But no specific tools that Congress needs to provide at this point in time to OMB to improve cost estimating practices? I mean——

Ms. MARTORANA. I think I would look forward to working with you and your staff and continuing to have a conversation about that.

Mr. KELLER. OK. Thank you. I yield back.

Mr. CONNOLLY. Thank you, Mr. Keller.

I would just observe that the witness said something I think that is really important that goes to part of your question, and what Mr. Hice was getting at earlier.

Cybersecurity is not a separate topic compartmentalized from the IT system in place. If you are working on a legacy system, many of them were developed long before encryption was developed and they aren't adaptable or not easily adaptable. They are vulnerable systems.

That is why our effort here at modernizing IT is directly related to cyber capability. They are not separate subjects, and I think your question gets at that. And I really appreciate the answer the CIO of the Federal Government, because that often gets over-looked. Thank you so much.

The gentlelady, our vice chair for this subcommittee, Ms. Porter, is recognized for her five minutes. Welcome.

Ms. PORTER. Thank you very much.

In June 2019, about two years ago, the Office of Management and Budget issued a memorandum that updated the reporting re-quirements for Federal data centers. Among other things, this guidance redefined the data center as a purpose-built physically separate dedicated space that meets certain criteria.

And as a result, agencies have excluded about 4,500 data centers from their inventories.

Ms. Harris, is OMB's current guidance on Federal data centers in compliance with FITARA?

Ms. HARRIS. The short answer is no.

Ms. PORTER. I will take the short answer, Ms. Harris, because I get them so infrequently in Congress. Is OMB's current guidance a good practice from a cybersecurity standpoint?

Ms. HARRIS. Well, I mean, I think that from a cybersecurity standpoint, there are other vehicles in place that may be able to address the cybersecurity risk exposure on the data centers.

So, I think the larger concern that we have in terms of dropping the non-tier data centers is our ability to have transparency and be able to track these centers and be able to stay aggressive in con-solidation efforts, because there is still money that we are leaving on the table here.

So, from that perspective and also an optimization perspective, too, ensuring that these centers are fully optimized. We are not able to get that if we don't have a better idea of what is in the in-ventory.

Ms. PORTER. And following this subcommittee's FITARA 10.0 hearing, OMB submitted responses to the chairman's questions for the record on this data center guidance, and in its response to the question about this change in the data center definition, OMB stated that they, quote, "removed requirements and reporting to align with industry standards, while also reducing the reporting burden that was time consuming and expensive."

OMB also said to focus on data centers deemed to be key mission facilities.

Ms. Harris, in GAO's work, have you seen non-tier data centers that are key mission facilities?

Ms. HARRIS. Well, we certainly want to—I think that there is a middle ground here. I think the pendulum has swung a little too far in terms of what we have omitted in the data center inventory—or the data center definition.

But we don't necessarily want or need to track individual desktops. I think that from a reporting perspective, that is burdensome to the agencies. But we also——

Ms. PORTER. Reclaiming my time, Ms. Harris.

I think you are exactly right. So, I want to point out some of what is being left out. Since OMB issued its guidance, the State Department data center reporting has dropped by more than half.

And you are right, we don't need to track every laptop. But, for example, State Department no longer reports on two 10,000-plus-square-foot facilities.

The Social Security Administration, Mr. Brune, has seven facilities between 4,500 and 9,600 square feet that are no longer subject to these reporting requirements.

You mentioned the value of transparency. Why is transparency so important when we are talking about these significantly sized facilities?

Ms. Harris?

Ms. HARRIS. I agree with you. I think that is—the examples that you just mentioned are reasons why we should be reevaluating the definition of what constitutes a data center because we do want to keep track of some of the non-tier data centers, particularly the fairly big ones that you just identified, and make sure that they are, you know, following the requirements of the DCOI initiative and are subject to the—you know, the reporting requirements associated with that initiative.

Ms. PORTER. Thank you very much, Ms. Harris.

I think that is extremely helpful.

Having heard what you have to say, Ms. Martorana, will you commit to working with this subcommittee to ensure proper oversight and transparency into these significantly sized, mission-critical, non-tiered data centers?

Ms. MARTORANA. Thank you very much for that and I will make—give you another easy answer. Yes, I will commit to continuing to have that conversation and working——

Ms. PORTER. This my lucky day. I rarely get two yes and no's in the same hearing. I feel very, very blessed to be participating in this today.

I think it is really important that the American public understand that the lack of transparency makes it impossible to fully

protect taxpayer money and ensure that agencies are tracking all potential security vulnerabilities.

So, I really appreciate OMB stepping up here and committing to doing what they can to not leave money on the table, to not leave us exposed to cyber attacks, because agencies simply find it difficult sometimes to follow best practices and the law.

Thank you very much, and with that, Mr. Chair, I yield back.

Mr. CONNOLLY. Ms. Porter, thank you for your questioning, and let me just say you are a person after my own heart. Before you joined us, this was the subject I focused on and made it very clear that this subcommittee is going to insist on the letter of the law being complied with.

And I would say to Ms. Harris while we are not unsympathetic with the need for some latitude in exercising judgment, the idea of it is a burden to an agency to comply with the law you will find us most unsympathetic to that and we would expect your agency to be similarly unsympathetic to that.

When we pass a law, we expect it to be complied with. The time to argue is while we are debating that draft legislation, not after it becomes law.

And Ms. Porter is absolutely right. Transparency is affected. Compliance with the law is affected. And I can just tell you, the fact that we have had 12 hearings on this subject all about compliance with the law—no other committee in Congress that I am aware of has ever done that—I hope demonstrates our determination to insist that this happen.

We see ourselves as your partner, but we are going to insist that the various components of FITARA that Mr. Issa and I wrote be complied with, and we are prepared to pass more legislation on a bipartisan basis, if necessary.

So, Ms. Porter's points are very well taken. There is a difference between some latitude and a desire to circumvent the law. Those are two different things. And we are—I said at the outset of this hearing we are concerned about that word, optimization, because it is a euphemism, we fear, for circumventing the requirement of the law, and that we are not going to go along with it. And that is not a new message from this subcommittee on a bipartisan basis.

So, Ms. Porter, thank you. You have made the point and very well, and we really appreciate the commitment coming out of OMB as we move forward.

Mr. Issa, you are recognized. Welcome back.

Mr. ISSA. Thank you, Mr. Chairman. And as you said, this is an area where you and I had the opportunity to work together for multiple years.

And if I can pick up where you just left off, Chairman, where Ms. Porter just left off, the intent—what you worked in a bulldog type way for years on was to reduce the total number of distinct facilities that had to be managed, many of them having the basic problem of telling us they weren't large enough to be managed properly.

But in a cloud world, there is only one server farm because every farm is connected. If there is only one server farm, that—as Ms. Porter said, that 4,500-square-foot facility that is not reporting could, in fact, be the weak link within a single cloud that has dozens or hundreds of locations.

But at the end of the day, the bad guys only have to make a cyber penetration in one place. So, the very existence of those small facilities and then a claim that they cannot have the same level of transparency and perhaps not the same level of professionalism begs the question, why do they exist at all?

And I want to commend the committee for continuing to work on that and for holding this hearing today.

Ms. Harris, I have got a longer reaching one, a question you were not probably prepared for. But as Congressman Connolly and myself envisioned modernization under FITARA, we created the very positions or at least gave them real strength of these CIOs.

They were created and given power and a direct link to, essentially, their cabinet head or agency head because of a history of not having the kind of professionalism overseeing $100 billion-plus in expenditures and, ultimately, the $4 or $5 trillion of government spending that depend on it, and then at the end of the day, $22 or $23 trillion of the American economy that, as we know, can shut down if portions of the government become inoperative.

Therefore, the question I have for you as our agency is, isn't it time for us to consider looking at stringing together this network of CIOs and, particularly, as to cyber into a single point of accountability, similarly to the Office of Personnel Management, the Office of Management and Budget, or any other cabinet head?

Isn't it time that the government accountability and the government ops, which is our committee, Mr. Connolly's committee now, isn't it time that we look at a reorganization that takes that $100 billion plus dollars and creates at least one person accountable directly to the president who has the expertise to—and the vision to bring together these disparate entities that are spread across the government?

Ms. HARRIS. Yes, I think that is a—that is what is needed, because when you look across the agencies with, you know, the proliferation of CIOs, it dilutes accountability.

And so having a single point of accountability is absolutely a great idea and I think would go a long way in improving IT management.

Mr. ISSA. Well, I am going to give each of the CIOs an opportunity to weigh in on some of their frustrations. But I would ask the chairman to consider tasking the Government Accountability Office with some further study on that to help the committee.

But if any of the CIOs want to weigh in on some of the frustrations they see by not having a higher level of person who has the kind of expertise that each of you has.

And maybe we start off with the Office of Management and Budget.

Ms. MARTORANA. It is an interesting question to ponder. I have not really given this an enormous amount of thought prior to the question. But I think that we are making an enormous amount of progress working across the Federal CIO community in an incredibly collaborative way.

We are working on several projects together that are enterprise in mindset so that we are not learning, you know, each one starting from a blank piece of paper.

You know, this is—we think, as Federal CIOs, of cybersecurity and IT modernization is a team sport. This is not an endeavor that any of us takes on in a silo, thinking only of our own agency. We think about our fellow colleagues.

I know when I was a—an agency CIO, I was greatly benefited during the beginning of COVID by other CIOs who had gone on a journey well in advance of where my technology part—my technology team and infrastructure was.

So, I think this is a team sport. We are all working very collaboratively as CIOs. But I would look forward to continuing to work together on this——

Mr. CONNOLLY. Brief—thank you. Briefly, because the gentleman's time has expired, I want to give Mr. Bluestein and Mr. Brune an opportunity to respond briefly.

Mr. BLUESTEIN. Sir, I appreciate the opportunity to respond to that. I echo Ms. Martorana's commentary. First of all, the environment amongst the CIO Council—the government CIOs has been very collaborative and there are certain things we are trying to break down some of these barriers.

I think that that goes right to Congressman Issa's point about collaboration in cybersecurity, having—whether it is some cyber entity that oversees all that but can kind of break through some of those barriers.

FITARA has been realized in my agency. So, I don't want for those kinds of things, if you will, in my organization. But as we collaborate with other agencies, it would be nice in some cases if we could break down those silos while making sure that we are secure.

Mr. CONNOLLY. Mr. Brune, did you want to comment?

Mr. BRUNE. Thank you, Chairman, and thank you, Congressman, for the question.

I would say that the enterprise focus is growing. Recently, the Social Security Administration joined partnership with the General Service Administration and other agencies on registration authentication for secure online accounts.

The GSA administers a program, *login.gov*. We use that. So, it is done on behalf of the public and we can use—build it once, use it multiple times. That is just one example where the collaboration that the Federal CIO mentioned is occurring, and I see it growing.

Mr. ISSA. Thank you, Mr. Chairman. This has been a great, great pleasure, and I appreciate your indulgence for the extra minutes.

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

And I would just editorialize as a final thought, and it goes back to a comment you made, Mr. Bluestein, about, you know, the org chart and solid line versus dotted line and all that.

But Mr. Issa will remember that when we wrote FITARA, among 24 Federal agencies there were 250 people with the title of CIO.

Now, there is no private entity that would tolerate that. And even in writing the bill, we chose not to do it by fiat. We chose to hope that there would be an evolution, that somebody would emerge as the primus inter pares.

And the reason we have emphasized the solid line is because of this proliferation. Someone has got to be in charge. Someone has got to be designated as the responsible and accountable person who is empowered to make decisions.

And in bureaucracies if you do not report to the boss, especially public sector bureaucracies, everybody knows anything you have to say is ad referendum. I am using some Latin today. I am sorry. And that is what we are trying to get at, and if there is a better way to do it we would love to hear it.

But I think both Mr. Issa and I reflect on a private sector experience and look at the Federal Government and say this is a system that can't possibly work with that many people with that title.

So, that is—that is what we are trying to get at. I think you would concur, Mr. Issa. Yes. Thank you very much.

Mr. LaTurner, thank you for your patience. You are recognized.

Mr. LaTURNER. Thank you, Mr. Chairman.

Ms. Martorana, I would like to visit with you just a little bit about the Technology Modernization Fund. As you know, it was established by Congress in 2017 to provide agencies additional ways to fund IT projects in a timely manner.

Has the fund adequately lived up to its purpose?

Ms. MARTORANA. Thank you, Congressman, for that question.

I am so bullish on the Technology Modernization Fund, not only in the way that it has managed IT projects that it did during its kind of 1.0 phase. Now that we are in a 2.0 phase with the $1 billion in the American Rescue Plan funding. I have—I see just enormous possibility.

So, a couple things that really stand out to me is, one is the board of TMF are all government officials that are real subject matter experts. They take their responsibility as board members very seriously.

We are spending about 10 hours a week meeting and reviewing proposals currently. We have brought subject matter experts in where we feel that we might have an opportunity, as I mentioned earlier, to have a little more of a top-down view across the portfolio. So, that is making me incredibly optimistic about this opportunity.

The second is, the repayment flexibility that has been extended to agencies under the American Rescue Plan is having a meaningful impact on agencies' ability to participate in this, right.

Not all agencies have working capital funds. We know that that is continuing to evolve. But it was really a barrier of entry for people being able to participate in TMF. With the repayment flexibility loosened a bit, that has made all the difference in the world, and we know that this will continue to have an impact.

The third reason that I am really optimistic about TMF is we are using best practices in how we are reviewing projects, awarding proposals to move forward, and managing them.

There is quarterly meetings with the TMF board to review progress. We only give out funds on an incremental basis based on accomplishments, milestones being met.

And we are also taking corrective actions when we see that a project is not fulfilling where milestones or where we think it should be.

We are bringing in subject matter experts, again, to partner with those agencies on corrective actions and we are willing to stop funding should we not believe that an agency is going to be successful.

So, we believe that TMF is going to have improved outcomes in the IT projects that we are funding and we hope to be able to continue to demonstrate that to the committee and to Congress.

Mr. LATURNER. I appreciate that. I have some additional questions on that but I am going to run out of time. Specifically, that my understanding is that there is $10 billion of the $60 billion for Fiscal Year 1922 in the request that has been earmarked for cybersecurity.

Could you drill down into that a little bit in the time that we have left and talk about how those funds will be allocated and spent to strengthen our cybersecurity?

Ms. MARTORANA. Yes. Out of—I can speak specifically to the TMF proposals that had a primary, secondary, or tertiary cybersecurity component.

We asked agencies to self-identify when they were submitting a proposal. Forty-two percent of the proposals are modernizing high-priority systems, and that is—those are oftentimes mission-critical systems that are operating our Federal Government.

So, 42 percent are focused on upgrading, updating, and increasing the cybersecurity posture of high-value systems.

The next are squarely cybersecurity requests, agencies that are coming to us and saying that they would like to begin on the road to more modern security practices like zero trust, which is a framework for not trusting anything inside your environment and making sure that you are rigorously interrogating everything within your boundaries.

It is actually eliminating boundaries. I won't get too technical. But we are focused on that, and so about 75 percent of all requests into TMF through the American Rescue Plan are focused on cybersecurity.

Mr. LATURNER. I appreciate that. It is such an important subject that I would love to spend more time on. But my time has expired.

Thank you, Mr. Chairman. I yield back.

Mr. CONNOLLY. Mr. LaTurner, thank you, and let me invite you, if you do have followup questions please get them to my staff and we will forward them to the appropriate witness.

Mr. LATURNER. Thank you, Mr. Chairman.

Mr. CONNOLLY. There is that opportunity, if we can do it within five days, and we ask our witnesses to be as expeditious as possible but as thorough as possible in responding to written questions, because, obviously, we can't ask everything in the hearing. So happy to do that, Mr. LaTurner. Thank you.

And if I can close out this hearing with some questions of my own, but I want to—Mr. Bluestein, I want to focus on you for a minute because I think you joined the agency in June, but the avalanche for SBA occurred in April and May.

So, we signed the CARES Act, big bipartisan bill. A lot of money for it. It was starting a new program, the PPP, and what we did that, I think, put a burden on SBA, and you rightfully pointed out the magnitude of scale.

So, I think your annual loan portfolio is something like $20 billion a year. We gave you $600 billion in one month. We also lessened the requirements for eligibility. We really streamlined them. We reduced paperwork.

We reduced documentation requirements because we were panicked, right. We wanted to get help to Main Street mom-and-pops as quickly as possible so they didn't go under. A noble goal.

And we also had a—that program had a provision that allowed loans to be converted to grants fairly easily.

Now, in doing all that with great intentions, we were relying, in a sense, on the SBA IT system e-TRAN.

And what happened in the first few weeks—oh, we added—I am sorry. One other change, which was a big one, we broadened the financial institutions eligible to manage the portfolios. We wanted to get into communities, including communities we were targeting—low income, communities of color—and that meant we had to look at community-based financial institutions, not the normal financial institutions that normally are the go-to managers of SBA's portfolio.

And what we found was that your IT system could not handle that. It couldn't—it had trouble programming the changes. It had trouble managing a huge avalanche of new money in a new program and it was overwhelmed by the demand.

And I am not citing that to criticize SBA. I cite it as an example of why IT is so important, because no one could have foreseen these circumstances. But our whole mission up here was shared by your agency, which was rush aid—run, don't walk to get aid to these small businesses so we are saving them and they are not going under, and while at the same time, we will have a condition keep people on the payroll. That is the goal here. We want to keep you open and we want to keep those people on payroll so we are not adding to the massive unemployment, which we were experiencing in April 2020.

But if you don't invest in the IT system to have the agility and the flexibility for these kinds of changes, how can you be surprised that it is overwhelmed and your mission is defeated? Not by some nefarious, you know, person or persons wanting to muck up the works, but because the IT system can't do it.

How often do we have to be reminded how critical and integral the IT system is to the mission? And we see that in unemployment insurance systems across the country, in the 50 state unemployment insurance systems.

We see it at the IRS in getting payments. We are changing the IRS mission, in a sense, or broadening it, from a tax collector to, you know, a benefit agency, and we are a little surprised that it has some trouble and its IT systems are older and more multiplicitous than yours.

I just want to give you a chance to kind of—because you came in June after all that happened and you were kind of in the cleanup operation. But I am sure you have some reflections about the good, the bad, and the ugly and what we have learned from that kind of experience.

And then I will be done.

Mr. BLUESTEIN. Thank you for the opportunity to comment on that, sir.

I did come in after the fact. One of the first things we did was we took a look at the entire ecosystem, because they were different systems that handled the PPP loans and the EIDL loans, and they

were—while they were somewhat disconnected, they still ran through the same system of systems that managed the capital access process.

So, one of the first things we did is say let us take a look at this end to end. How do you streamline all of this so it operates on some kind of plane, and let me diverge for just a second.

When all of this happened last year and there was a Presidential tweet that said *sba.gov*, our website that normally handled about 600 to 700 concurrent users went to 93,000 in a matter of minutes.

Now, that was all set on a modern platform that immediately scaled to handle from about one terabyte a day of data to about 25 terabytes a day. So, it was built to scale.

And we want to bring that same technology into these financial systems. Unfortunately, a lot of times in risk management until we actually realize the risk—people talk about it, but they won't take necessarily the measures to fix that.

Now we have been in a situation where we saw the consequence, and especially with all the different things that have happened subsequent to that—different requirements, how do we slice and dice some of these things to discreetly identify either communities of interest, other things that we want to do in the system—that technology is available out there.

We are going through the process now of figuring out, OK, what do we do with the system that we have? We have e-TRAN, which has been there. It is legacy code. We know it.

And the next step is, OK, how do we move beyond that. We are working very, very closely with the capital access folks to work through that.

Mr. CONNOLLY. Thank you so much, and I look forward to having further discussion with you about what happened and what we can take away, sir, because I think all of us benefit from that experience in terms of—and I would commend to you, Ms. Martorana, on your agenda many things to get done.

But I really would look at lessons learned from the pandemic in terms of IT because I think we could really, all of us, benefit from that. There were some great things. There were some things that didn't work, some things that were disasters, and some things we could have done better.

The TMF is in that context, I think, as you were saying earlier in terms of how we might use it to help upgrade, to help people make other investments, better investments. But I do think there are some very critical lessons to be learned from this experience, and you might very well want to take the lead on that.

And I think Mr. Issa suggested, Ms. Harris, that I might want to join him in urging you to look at a couple of issues, and Mr. Hice also, and I gladly nod yes to add to your plate.

Mr. Hice, anything for the good of the order you want to add?

Mr. HICE. I don't. I am——

Mr. CONNOLLY. Yes, no problem. You are going to mischief.

[Laughter.]

Mr. CONNOLLY. All right.

I want to thank our witnesses, and again, any member wishing to add—to submit written questions for the record, we will be glad to provide them to our witnesses.

I think this has been a thoughtful dialog. Really appreciate the work of everybody involved. I think you can see our commitment. I know it is not the sexiest topic in the world.

But to me, IT undergirds everything we are trying to do in the mission, and the mission is jeopardized if the IT doesn't work. And we have the added layer of being really concerned about cyber and how do we protect ourselves.

And as Ms. Martorana, I think, astutely observed, the two are linked. If you have got an old clunky antique legacy system that cannot be encrypted or cannot easily be encrypted, you are asking for trouble, and that is why making smart investments that are cyber protected and that also take advantage of the most advanced technology better serve our constituents and protect their privacy and their interests and the national security, while we are at it.

With that, this hearing is adjourned.

[Whereupon, at 3:52 p.m., the subcommittee was adjourned.]

○