FITARA 10.0

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

AUGUST 3, 2020

Serial No. 116–110

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
41–910 PDF WASHINGTON : 2020

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
RO KHANNA, California
KWEISI MFUME, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan
KATIE PORTER, California

JAMES COMER, Kentucky, *Ranking Minority Member*
JIM JORDAN, Ohio
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida
FRED KELLER, Pennsylvania

DAVID RAPALLO, *Staff Director*
WENDY GINSBERG, *Subcommittee Staff Director*
CAMERON MACPHERSON, *Clerk*
CONTACT NUMBER: 202-225-5051
CHRISTOPHER HIXON, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

ELEANOR HOLMES NORTON, District of Columbia
JOHN P. SARBANES, Maryland
JACKIE SPEIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
RO KHANNA, California
STEPHEN F. LYNCH, Massachsetts
JAMIE RASKIN, Maryland

JODY B. HICE, Georgia *Ranking Minority Member*
THOMAS MASSIE, Kentucky
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
RALPH NORMAN, South Carolina
W. GREGORY STEUBE, Florida

C O N T E N T S

INDEX OF DOCUMENTS

Documents listed below are available at: docs.house.gov.

FITARA 10.0

Monday, August 3, 2020

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

The subcommittee met, pursuant to notice, at 2:04 p.m., in room 2154, Rayburn House Office Building, Hon. Gerald E. Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Lynch, Raskin, Hice, Grothman, and Palmer.

Mr. CONNOLLY. Welcome, everybody, to the Subcommittee on Government Operations and our tenth hearing on FITARA.

Before we begin, pursuant to House rules, most members today will appear by Webex, remotely. Since some members are appearing in person, or at least this member is, let me remind everyone that pursuant to the latest guidance from the House Attending Physician, all individuals attending this hearing in person must wear a face mask. I'm dropping mine only to speak. Members who are not wearing a face mask will not be recognized.

Let me also make a few reminders for those members appearing in person. You'll only see members and witnesses appearing remotely on the monitor in front of you when they are speaking in what is known as Webex active speaker view. A timer is visible in the room directly in front of you.

For members appearing remotely, I know you're all familiar with Webex by now, but let me remind everybody about a few points. First, you will be able to see each person speaking during the hearing, whether they're in person or remote, as long as you have your Webex set to active speaker view. If you have any questions, contact Committee staff and they will try to be helpful.

Second, we have a timer that should be visible on your screen when you're in the active speaker with thumbnail view. Members who wish to pin the timer to their screens should contact Committee staff for assistance.

Third, the House rules require that we see you, so please have your cameras turned on if you're on remotely on Webex during this hearing.

Fourth, members appearing remotely who are not recognized should remain muted to minimize background noise and feedback.

Fifth, I'll recognize members verbally, but members retain the right to seek recognition verbally in regular order. Members will be recognized otherwise in seniority order for questions.

Last, if you want to be recognized outside of regular order, you can identify it in several ways. You can use the chat function, you can send an email to majority staff, or you can unmute yourself to seek recognition verbally, though that's the least preferable way to do it. Obviously, we don't want people talking over each other.

Let's see. OK. I will begin with my opening statement.

Mr. Hice, you are on remotely?

Mr. HICE. Yes, sir, I'm here.

Mr. CONNOLLY. OK. We're glad you're there. I know you're in self-quarantine, and I know you'd prefer to be here physically, but I am really glad we have the hybrid remote option so that you can participate fully in today's hearing, and hope everything's going to be OK. And I'll call upon you as soon as I finish my opening statement for any remarks you may have.

Today marks the tenth hearing examining agencies' implementation of the Federal Information Technology Acquisition Reform Act, known as FITARA, to track agencies' progress in Federal management and procurement.

I'm happy to announce that this steady oversight has produced the first scorecard in which all agencies received a passing grade. This achievement is a testament to the hard work of Federal agencies' Chief Information Officers, and also a testament to, I think, this committee and subcommittee's steady and bipartisan oversight of FITARA since we enacted it in 2014.

This isn't just about passing grades. These grades represent taxpayer dollars saved, better mission delivery, and serving the Nation more effectively and efficiently. And during this pandemic, we've come to realize just how vital good IT and strong IT governance are to Federal Government and the people we serve.

We certainly have seen limitations because of lack of IT investment, whether it be with the Ethernet system at SBA, Small Business Administration, or the struggles of the IRS to provide personal checks to all citizens and dependents in America. We've also seen limitations in the unemployment systems in the 50 respective states. So, it underscores how important these investments in this kind of improvement really are.

In November 2015, when we first introduced the FITARA scorecard, I said I hoped this would be the second in a series of hearings our subcommittee holds to gauge agency progress in realizing the transformative nature of FITARA's reforms. Five years later, the benefits of continued oversight, I think, are clear, and one would be hard-pressed to find a sustained bipartisan congressional oversight initiative on its tenth installation. These 24 agencies have made real improvements on the scorecard—and I think we're putting it up over there on that screen—over a period of time.

In November 2015, the average FITARA grade was a D across all participating agencies. This year, for the first time, no agency received a D and no agency, of course, received an F. As I said before, these improvements represent vital services delivered and dollars saved.

Among the FITARA scorecard categories with the greatest impact is the IT portfolio review process known as PortfolioStat. This process enables agencies to reduce commodity IT spending and demonstrate how IT investments align with the agency's mission

and business function. PortfolioStat went from helping Federal agencies save $3 billion in fiscal 2015 to $20 billion this fiscal year.

When the software licensing metric was first added to the scorecard in June 2017, 21 out of 24 agencies received an F grade for that metric. Now, 23 out of 24 agencies have As and have an inventory of software licenses and use that inventory to make cost-effective decisions and avoid duplications.

Federal agencies are also closing and consolidating more data centers, resulting in significant cost savings. The 24 graded agencies have a reported total of $4.7 billion in cost savings from fiscal years 2012 through 2019. Those agencies have also reported plans to save more than $264 million in this Fiscal Year alone.

At the very first FITARA hearing, a witness stated that IT is no longer just the business of the CIO; rather, IT is everybody's business. Never has this been clearer than in the wake of the coronavirus pandemic, where IT has saved thousands of lives by enabling people to telework and keep the government and the economy running while preserving their own health and safety. We have seen firsthand how the agencies that continued to use outdated IT during the pandemic prevented the delivery of government services when the public needed them most.

Back in 2015, I cautioned that the FITARA scorecard was not to be considered a scarlet letter but a point-in-time snapshot to be able to measure progress and incentivizing. Five years and ten scorecards later, we're now at a point in time where all agencies have received passing grades, the first time ever. FITARA 10.0 marks the point at which we can reflect on five years' worth of progress.

Initially, the FITARA scorecard consisted of four metrics, including data center consolidation, IT portfolio review savings, incremental project development delivery, and risk assessment transparency. Since then, the scorecard's success has led this subcommittee to incorporate other aspects of Federal IT into the grades.

Our framework is not rigid, but like the best of IT, it evolves. We augmented and changed the scorecard to examine other key components, such as cybersecurity, and incorporated constructive feedback from agencies and CIOs. Today, the scorecard incorporates grades adapted from three additional pieces of legislation, including the MEGABYTE Act, the Modernizing Government Technology Act, and the Federal Information Security Management Act.

The bottom line is that the FITARA scorecard continues to hold agencies accountable and show the American people that they deserve the best IT has to offer, yet all agencies still have work to do. Today, two-thirds of graded agencies have CIOs who report directly to the head or deputy of the agency. It's true that more CIOs are finally getting a seat at the table with other C-suite positions, but we'll hear from GAO today none of the 24 graded agencies have established policies that fully address the role of the CIO, as called for by Federal law and guidance. We must continue to work to ensure that all CIOs have the authority and policies in place to be able to properly do their jobs.

This hearing will discuss which existing metrics have achieved their goals and which might need to be considered for retirement.

We'll also start a careful discussion about what metrics might be incorporated in future scorecards to continue to improve IT across the government. In other words, we're going to continue this scorecard.

Today I hope to hear from our witnesses at GAO about what it takes to continuously improve and use efficient IT acquisition and management practices to do that, what powers and authorities might CIOs and government need to improve government IT, and in return, what transparency and oversight will be provided to Congress and the public to ensure those new powers are used effectively and efficiently. We must continue to see the dividends from putting resources toward modernizing legacy systems, migrating to the cloud, and maintaining a strong cyber posture.

With the coronavirus resurging as states pursue reopening, the stakes for effectively implementing FITARA are perhaps higher than ever. When executed well, government IT modernization can ensure the efficient delivery of critical services, improve the government's knowledge and decision-making, and save lives. When executed poorly, it can, unfortunately, lead to outright failures in serving the American people when they need the government the most. Simply put, the fate of the world's largest economy, it's no exaggeration to say, rises and falls with the ability of 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 will continue its oversight of agencies' IT acquisition and management as we move forward.

With that, I call upon the ranking member for his opening statement.

Mr. HICE. Thank you, Chairman Connolly, and thank you for holding this hearing today on the tenth FITARA scorecard. As you well know, this has literally been a bright spot of bipartisan work for this committee, and I look forward personally to continuing to see the development of the scorecard's usefulness as it relates to Federal IT reform.

I also would like to take just a moment and give a shout-out of thanks to the outgoing Federal Chief Information Officer Suzette Kent. She's been extremely dedicated in her service, is deeply appreciated. As you well know, enhanced CIO authority is one of the pillars, literally, of the FITARA, the whole system, and Ms. Kent has just done an outstanding job with her leadership and enthusiasm to really help drive some of the IT modernization efforts that have been outlined in the President's management agenda. So, we're grateful for her leadership and service, and hope to continue to buildupon the initiatives that she has championed.

But, as you shared, Chairman, we are here today to discuss the tenth FITARA scorecard. Agencies have really made tremendous progress, as you well mentioned, over the past five years, and I want to congratulate them on their dedication to improve the IT procurement and management processes. A job well done.

Some of the things that we have seen accomplished over the last several years include, as you mentioned, Mr. Chairman, savings of literally billions of dollars. We have increased transparency for risky IT investments and, of course, the elevation of the CIO position and authority within the agency.

So, for all these successes, we are very grateful for what has been done, but obviously, there is more yet that needs to be accomplished. And I would suggest some of those things, we need to continue to update the metrics so that they better and more effectively match the IT management and implementation practices that are actually being used today.

Also, I think it's imperative that we, as a committee, put in place the right kind of incentives to bring about IT modernization at scale as it relates to the pandemic. I think this has really highlighted to us and exposed, if you will, the heavy reliance that we have on some legacy systems and some longstanding technology problems. We need to find ways to get agencies to move the needle on some of these crucial issues.

And I think last, we need some forward-looking, if you will, some forward-looking metrics to help modernize government as a whole. I think some of those things would include some moving forward as it relates to the citizen experience. I think you actually referred to that, Mr. Chairman. I think it's important that we move in that direction, enhancing the skills of the Federal IT work force I think we need to continue looking toward, and also just overall moving toward a more agile and secure cloud computing environment. All these things I think are extremely important that we continue moving toward.

So, I look forward to hearing from our witnesses today. And in advance, I want to say thank you to each of our witnesses for being here today. We appreciate your time and your expertise that you'll bring to the table.

With that, Mr. Chairman, I will yield back. Thank you, sir.

Mr. CONNOLLY. Thank you, Mr. Hice. And I also want to thank you personally. You and I have talked about this. This subcommittee has always had a strong bipartisan thrust, especially on this subject. I worked closely with Darrell Issa in writing FITARA. I worked closely with Will Hurd in expanding on it and having these hearings on the scorecard, as well as with Mr. Meadows, now the chief of staff to the President of the United States. And you've pledged to do the same, and I really very much appreciate that and look forward to continuing to work with you, and hope you are OK and healthy in Georgia. Thank you for your remarks.

Ms. Harris, if you would unmute yourself in order to be sworn in, and if our three witnesses who are here in person would rise and raise their right hands.

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?

Let the record show that all of our witnesses answered in the affirmative.

Without objection, your written statements will be part of the record.

I now call on Carol Harris, director of IT Management Issues at the Government Accountability Office, to give us her summary testimony. Welcome, Ms. Harris.

STATEMENT OF CAROL HARRIS, DIRECTOR, IT MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Ms. HARRIS. Thank you, Chairman Connolly, Ranking Member Hice, and members of the subcommittee. I would like to thank you and your excellent staff for your continued oversight of Federal IT management and cybersecurity with this tenth set of grades. It's been nearly 5–1/2 years since FITARA's enactment, and your scorecard has served as a good barometer to measure progress of its implementation.

During this time period, the agencies have made significant progress. In this latest scorecard, there is 1 A, 9 Bs, and 14 Cs. As you mentioned, this is the first scorecard in which all 24 agencies received a passing grade. This is huge, considering only seven agencies had passing grades in the first scorecard. In addition, the agency with the greatest transformation has been the Department of Education, moving from an F to a B-plus.

I'll focus my remarks on a lookback on the progress made since scorecard one, where things stand now, and where we need to go.

First, agency progress made. I'll start with incremental development. The number of major IT projects utilizing incremental development has increased from 58 to 76 percent. In addition, the level of transparency on the dashboard has improved, with 61 percent of major projects being reported as red or yellow, as compared to 24 percent with the first scorecard. We've also seen dramatic improvements in the agency's management of software licenses, going from two A's to 23. And the number of CIOs with direct reporting to the agency head has increased from 11 to 16.

To date, the agencies have also closed more than 6,300 data centers and saved just shy of $20 billion through OMB's PortfolioStat initiative. The progress made in all of these areas would not have happened to this extent without your scorecard and oversight.

While these accomplishments are indeed noteworthy, significant actions remain to be completed to build on this progress, and this brings me to my next point on where we're at.

One-third of the agencies' CIOs still aren't reporting to the agency head. CIOs have told us that this reporting structure is critical to carry out their responsibilities. It gives CIOs a real seat at the management table, and it will likely help to attract more qualified individuals to these positions over time.

In addition, about half of the agencies have not established working capital funds for use in transitioning from legacy IT systems. Roughly 80 percent of the over $90 billion spent annually on Federal IT is on operations and maintenance, including on aging legacy systems. Establishing these funds are so critical so that the savings from software licenses, data center optimization, and PortfolioStat can be reinvested in agency IT modernization priorities. If each of these agencies did these two things, the grades would be 4 As, 15 Bs, and 5 Cs. These two actions and the associated higher grades are achievable by the next scorecard.

Now turning to data centers. We remain concerned about OMB's current guidance which revised the classification of data centers and data center optimization metrics. For example, OMB's new data center definition excludes more than 2,000 facilities that agencies previously reported on. Many of these excluded facilities rep-

resent what OMB itself has identified as possible security risks. The changes will likely slow down or even halt important progress agencies should be making to consolidate, optimize, and secure their data centers.

Finally, regarding where we need to go scorecard-wise, the preview of the Federal EIS telecommunications transition will draw urgent attention to an area that has historically been neglected by the agencies. For example, had the prior telecom transition occurred on time, agencies could have saved $330 million. And as I testified before you earlier this year, the agencies are behind schedule and could again be missing out on hundreds of millions in savings. Your scorecard will be an effective means for holding agencies accountable and ensuring a timely transition.

Mr. Chairman, this concludes my comments, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Ms. Harris, and I look forward to those questions as well.

Clare Martorana. Have I got that right, Clare?

Ms. MARTORANA. Close, sir. Martorana.

Mr. CONNOLLY. Martorana, forgive me. You are recognized for five minutes.

STATEMENT OF CLARE MARTORANA, CHIEF INFORMATION OFFICER, OFFICE OF PERSONNEL MANAGEMENT

Ms. MARTORANA. Chairman Connolly, Ranking Member Hice, members of the subcommittee, thank you for the opportunity to discuss the status of information technology at the Office of Personnel Management, and to provide thoughts on the future of FITARA.

I joined OPM in February 2019 as the seventh CIO in seven years and entered an agency with several key challenges: Critical staffing vacancies, antiquated and fragile technology, and a charge to fully transition the IT systems for National Background Investigation Bureau, now DCSA, to the Department of Defense, which we hope to complete this fall.

As a new Federal CIO coming from the private sector, admittedly, this is a complex operating environment. Meeting and balancing numerous executive, legislative, and oversight requirements while working in an uncertain and inflexible budgetary cycle is quite challenging. However, I'd like to focus on what's possible, because that's what OPM's employees and the American people deserve.

One of the first authorities I learned about was FITARA. As CIO, it provides me with an operating framework and a mandate to make enterprise IT decisions and strategic investments that make best use of taxpayer dollars. I have received a steady stream of support from OPM leadership and—I'm sorry. I have received a steady stream of support from OPM leadership to meet the provisions of FITARA by establishing an agencywide enterprise IT strategy. We anticipate working with program offices and enabling organizations as we move forward in this direction.

We are extremely proud of raising OPM's FITARA score to a C-plus. With only one net new hire and no increase in incremental funding, we have been able to make significant progress and show people within OPM what is possible, like rolling out new laptops

across the organization and moving to cloud email. This has enabled us to continue meeting our mission while supporting DCSA employees and contractors in a maximum telework environment during the pandemic.

Just a few weeks ago, the dedicated CIO team successfully migrated our mainframe platform from the Teddy Roosevelt Building here in D.C. to a commercial data center. OPM and DCSA systems are now fully operational in a new modern environment with continuity of operations in place. Once we transition the daily IT operations of this important national security mission to our colleagues at the Department of Defense this fall, OPM will be able to focus on OPM's mission and begin our digital modernization journey.

Now I'd like to touch on a few enhancements to FITARA that could drive digital modernization at OPM and across government. The first is funding flexibility. OPM's legacy funding model with seven funding streams for CIO creates incredible complexity and inflexibility to address our IT challenges. By standing up a working capital fund with transfer authority dedicated to IT enterprise investment and CIO oversight and authority over this funding, we will create enterprise efficiencies and measurable cost avoidance.

Also, modern technology, because Federal employees deserve the tools I've had the benefit of using in the private sector. Attracting, retaining, training and reskilling our work force with a customer-first mindset, utilizing agile development, modern tools, and modern technology is essential.

Our modernization strategy begins with upgrading our existing paper-based processes and workflows with modern electronic equivalents, allowing us to retire end-of-life systems. All of these are possible if we work on modernizing OPM together and giving OPM's customers the 21st century experience that they deserve.

I look forward to working on this digital modernization journey together. Thank you for the invitation, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Ms. Martorana. Martorana. Martorana, excuse me.

Mr. Jason Gray, Chief Information Officer of the Department of Education, you are recognized for five minutes.

STATEMENT OF JASON GRAY, CHIEF INFORMATION OFFICER, DEPARTMENT OF EDUCATION

Mr. GRAY. Thank you, Chairman Connolly, Ranking Member Hice, and members of the subcommittee, for this opportunity to appear before you today to talk about the progress the Department of Education has made in implementing FITARA. I would also like to thank you for your continued support and commitment to improving IT management across the Federal Government.

I appreciate the support I received from Secretary DeVos and Deputy Secretary Zais. It has been critical to the Department's FITARA implementation. I also want to thank my colleagues in Federal Student Aid, the assistant secretaries, and everyone in my office for their continued hard work, commitment, and dedication.

I'd like to briefly share an update on our IT modernization efforts and describe the impact FITARA has had on my ability to effectively manage the Department's IT.

In my June 2019 testimony before this committee, I shared that the Department had just completed a massive wholesale modernization of our IT infrastructure. This effort transformed the way my office delivers IT services to the Department. Within a five-month timeframe, we migrated over 450 terabytes of data into a secure cloud environment and replaced approximately 5,000 laptops with newer high-performing models. Our users went from experiencing 20 minutes of laptop boot-up time to less than a minute, which translates into a return on investment of more than 1,500 hours of previously lost productivity per day.

The cloud environment enabled us to reduce the Department's service storage cost from $1.43 per gigabyte to 12 cents per gigabyte. The Department anticipates saving approximately $20.5 million over a five-year period as a result of this initiative.

While the Department will realize cost savings, the true value of the modernization initiative was in our ability to quickly adapt and respond to the Department's needs throughout the pandemic. Due in large part to the modernization, we have been able to support 100 percent remote work force with minimal impact. When our PIV issuance process was suspended due to staff not being able to come into the office, we were able to quickly evaluate and implement within days, not months, a solution to virtually onboard more than 300 new employees and contractors to date.

By fully embracing the cloud, we were also able to complete a massive technology refresh of 28 major systems, more than 700 servers, and over 500 terabytes of data over a single weekend, with no impacts to IT services. In a traditional environment, this would have taken us weeks to accomplish. Without FITARA, we would not have been able to complete the massive IT modernization initiative last year and certainly not within the timeframe I described.

It was through the reporting relationship I have with Secretary DeVos and the relationships we have built across functional areas that I was able to drive the Department's IT priorities to achieve our IT modernization goals. The initiative was a cornerstone of our five-year IT modernization plan and strategic roadmap, and I'd like to thank you for providing us with the opportunity, following my testimony last year, to brief Representatives of this committee on it.

When we originally developed our modernization plan and strategic roadmap, we identified shadow IT, redundant or duplicative systems, and manual or obsolete processes. The institutionalization of FITARA in the Department's governance process has provided me with the mechanisms to continually assess and rationalize our IT portfolio and adjust our plans accordingly, from strategically aligning our IT resource management plans with the requirements of the Foundations for Evidence-Based Policymaking Act of 2018 to prioritizing investments to comply with the 21st Century Integrated Digital Experience Act, or evaluating the use of shared services for capabilities such as grants management to the rapid response actions required to address emergency cybersecurity directives from DHS. I am able to achieve a level of visibility necessary to understand the impact to Department's IT resources.

While we have made significant strides in our FITARA maturation and IT modernization initiatives, the Department continues to

seek Congress' assistance with the establishment of a working capital fund. We coordinated with OMB and Congress to obtain appropriations language that would allow us to transfer funds to a working capital fund and included the request in our President's budget request for both 2020 and 2021. I respectfully request your assistance with obtaining this transfer authority to further enhance the Department's ability to achieve the goals of FITARA.

In conclusion, the Department has established a solid FITARA framework and have clearly demonstrated our ability to leverage it in support of the Department's mission. But we do recognize that FITARA and IT modernization is a journey and it's important to continually improve.

I thank you for your time today, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Mr. Gray. It's good to have you again giving us a year later progress. We certainly will try to work with you on that transfer authority, so work with us on that.

Our final participant in this panel is Maria Roat—is that correct?

Ms. ROAT. Yes, sir.

Mr. CONNOLLY [continuing]. Who's the Deputy Federal Chief Information Officer at the Office of Management and Budget. Welcome.

STATEMENT OF MARIA A. ROAT, DEPUTY FEDERAL CHIEF INFORMATION OFFICER, OFFICE OF MANAGEMENT AND BUDGET

Ms. ROAT. Thank you. Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you for the opportunity to discuss FITARA and how we can continue to drive and sustain governmentwide IT modernization.

I joined OMB eight weeks ago as the Deputy Federal Chief Information Officer, bringing a career of Federal and military technology experience and an agency perspective to my role. Throughout my career, I have seen firsthand the value of investing in modern scalable solutions and how taking prudent risk, collaborating, brainstorming, and sharing ideas and concepts drives change. And I have experience as a CIO and know how a strong partnership with and commitment from an agency's business stakeholders can improve how the government meets its mission and serves the American public.

COVID–19 put a spotlight on digital transformation and the need to adapt quickly. Every agency worked at never before experienced levels of telework and sustained performance by leveraging capabilities already in place. There was a sense of urgency, and CIOs were entrepreneurial, creative, innovative, and agile.

Since the first FITARA scorecard, technology investments in cloud, in infrastructure enabled an overall seamless transition to telework. Simultaneously, CIOs were positioned to rapidly deploy and leverage scalable platforms for digital service delivery for COVID response activities. They leveraged microservices to quickly stand up new public-facing portals and switched to video teleconferencing for telehealth and benefits interviews and to engage with their customers.

CIOs deployed virtual desktops to replace the purchase of costly hardware for surge employees. And the CIO Council identified areas for future investments and improvements where we need to address gaps or move faster. We must keep the momentum. Agencies were able to move fast, innovate, and implement changes for more digital interoperability. There is a shared interest across all levels of government, Congress, the executive branch and the administration, to continue technology improvements.

The Technology Modernization Fund and IT working capital funds and their multi-year funding approaches are two programs instrumental in improving, retiring, or replacing legacy systems. We must do more to drive sustained long-term transformation and ensure digital first as we add value and service delivery.

Throughout my career, I've had the honor to lead and work side by side with amazing innovators and technologists, public servants working for the Federal Government. Today, over 2 million civilian personnel use technology to carry out their job.

Just as importantly, as we consider any technology investment, we should also remember that the people charged with using those solutions must also be skilled in the use of technology. As the pace of capability and threat continues to accelerate, we must invest in our work force to keep their skills relevant.

The CIO Council continues to invest in the IT work force and is building on last year's success with the Federal Cyber Reskilling Academy to launch this month a similar training program in data science. This summer, we are holding, virtually, the third annual Women in Federal IT event, where women in leadership positions across the Federal Government share stories and provide on-the-spot mentorship and career advice to emerging leaders. We graduated two cohorts from the robotic process automation reskilling course, and in September, we will graduate 20 people from the CIO and CISO SES Career Development Program.

As we focus today on the tenth edition of the FITARA scorecard, we must adapt to the ever-changing technology landscape and, likewise, adapt the scorecard. I look forward to collaborating with you to further refine the scorecard to support sustained, long-term modernization and drive innovation.

Thank you for the opportunity to speak with you today, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Ms. Roat. I appreciate that. I find myself in agreement with everything you've said. It is good to learn that the administration has decided to embrace telework in light of the pandemic, given the fact that the administration was actually cutting back on telework the last two years.

And with respect to retiring legacy systems and the need for the Technology Modernization Fund, I also find myself in agreement, but we need the administration to make a robust request in the budget if we're going to make progress on the TMF.

The chair now calls on the distinguished Congresswoman from the District of Columbia for her five minutes of questions. Welcome, Ms. Norton.

Ms. Norton, are you there? Ms. Norton?

Mr. Lynch, are you there?

Ms. NORTON. I'm here.

Mr. CONNOLLY. You're there. OK, great. Sorry about that. Eleanor, just speak up a little bit.

Ms. NORTON. All right. I'm sorry. I punched the wrong button.

Mr. CONNOLLY. There you go. There you go.

Ms. NORTON. Thank you very much.

And, Mr. Chairman, I want to thank you for this annual hearing. It's very important to have been brought up to date, as you have allowed our witnesses to do.

Now, the FITARA says—and I'm quoting it now—that CIOs have a significant role in the decision processes of the management, governance, and oversight processes related to information technology. Well, I would have thought that they have a major role to play in an agency overall, and I understand that IT is now baked into policy design and implementation.

This question is for Ms. Harris. There are CIOs that do not report to agency heads and, of course, if they don't, they're unlikely to play that key role that we spoke about. Well, who doesn't and why don't all of them now report?

I think it was perhaps in your testimony or the testimony of one of you that one-third do not report to the agency head. I'd like to know why. I understand that there's a minus and a plus that you can look to see whether people are reporting, but I don't understand what determines or how agencies determine what this committee has long said would be helpful.

Ms. HARRIS. That's correct, ma'am. About one-third of the agency CIOs do not have direct reporting mechanisms to the agency head, and that is a problem, because agency CIOs have reported to us that that reporting structure is very critical to allowing them to carry out their responsibilities.

Ms. NORTON. Well, Ms. Harris, would you explain to the committee what would be the resistance so that we can work with agencies? Why would an agency not want everybody in the room?

Ms. HARRIS. Honestly, I think it, in large part, has to do with agency culture, and being able to change that culture so that the CIO does have that seat at the table is vitally critical. So, it's going to take work with the senior leaders within those agencies to empower those CIOs, change those organization charts so that those CIOs have direct reporting capabilities, and work with you all as well to ensure that that happens.

Ms. NORTON. I'd like to work with the chairman on making sure that there is no resistance. In the 21st century, you would have thought that having the CIO at the table would just be a given. So, I really don't understand the resistance to it, and believe that the committee could be helpful in either requiring, through legislation or through regulation, that the CIO be at the table.

This is a question, I suppose, for Ms. Roat, and it has to do with the recruitment of and attrition of IT staff. Are these staffers valuable outside of the public sector, Ms. Martorana or Ms. Roat? Is there great competition for these staffers? I'd like you to discuss that. Then I'd like you to tell the committee what we could do to help attract and keep Federal IT workers.

Ms. Roat?

Ms. ROAT. Yes, ma'am. Thank you for your question. For the work force, it is hard to attract work force to the Federal Govern-

ment and, in turn, folks that we do train in the Federal work force do go to the private sector and make more money.

What attracts people to the Federal Government is the ability to focus on a mission, whether you're working for the Department of Energy or Transportation or DHS or NASA. People are excited about the mission, and that's what draws people to the Federal Government. As a CIO, I've had experience with that where people want to come on board, and I've had some incredible talent. Other CIOs have had the same experience.

But to your question, it is hard to get people in, but once you get them in, the folks that want to come in, they want to stay. They love what they do. And when people leave the Federal Government, they may go back to private industry, get more experience, maybe they make more money, and then turn around and come back to the Federal Government.

But, again, we continue to explore flexibilities in hiring, compensation, and looking at ways to build skills. As I said in my opening comments, we've done a lot for the Federal work force so far through the CIO Council on data science, on cybersecurity, and we're going to continue to build on those skill sets so that we can maintain that work force. So, it's not only just attracting new workers, but maintaining and educating our current work force.

Ms. NORTON. Finally—I'd just like a moment, Mr. Chairman—is pay a salient issue here in keeping people in the Federal—IT workers in the Federal work force?

Ms. ROAT. For folks, for people that are working in the IT world that are coming into the Federal Government, they can get compensated much more on the private sector.

Ms. NORTON. We might have a look at that also, Mr. Chairman. Thank you very much. My time has expired.

Mr. CONNOLLY. Thank you, Congresswoman. And let me just say in response to your query about CIOs, I couldn't agree with you more. When we wrote FITARA, there were 250 people spread out over 24 agencies with the title CIO.

I asked the private sector, Ms. Martorana, how many CIOs do you have? And almost 100 percent the answer is one. So, we've got a lot of work to do. We didn't mandate there shall be one CIO. We allowed it to evolve that one CIO was sort of *primus inter pares*, first among equals, who reported to the boss. But if we need to strengthen that, we will. We'll also be guided, Ms. Harris, by GAO's counsel on that matter as well. But we are making progress.

And listening to the testimony today, you've got relationships with the head of the agency, and that makes all the difference in the world, the empowerment from the boss. But it's something we are very mindful of, and I thank the distinguished Congresswoman for bringing further attention to it.

The chair now recognizes the distinguished ranking member, Mr. Hice, for his five minutes.

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

Ms. Roat, I'd like to ask you this. One of the things that I have discovered in becoming more and more familiar with this, it seems like one of the current metrics measures how much of an agency's portfolio is high risk. The issue that I have found is that there's

no definition of what high risk is, at least not that I've been able to determine.

When I think of high risk, I think of things like vulnerability to cyber attacks, but what I found out is that high risk means something else to others. It may mean whether or not a system is able to be delivered on time and at budget and, if not, it's at high risk.

So, my question, really, is there any uniform and comparable kind of way for agencies to define what we all mean by high risk, so that we're all on the same page?

Ms. ROAT. Thank you for the question. As you look at the programs and the portfolios across the Federal Government, those programs that are high risk, GAO does look at programs that are high priority, the high priority programs, and there are different definitions, including high-value assets.

So, when you're looking at those systems that are at high risk, are those the systems that are the oldest in the Federal Government that perhaps need to be modernized or are they high-priority programs that are high visibility and have to be and are critical to the Federal Government. So, as we're looking at the definitions, there are separate definitions, whether it's high-priority programs, high-value assets that are critical to the Federal Government, or those programs and those systems that are high risk in the Federal Government. So, there are different characterizations that are used in different reports.

Mr. HICE. And to me, that's part of the problem. Is there any kind of way of getting a uniform understanding of what we're talking about on high risk? Because you just mentioned about three or four different things that come under that category. So, what—or even just to prioritize the high-risk categories so we know if the high risk is any of the things that you mentioned or if it's cyber vulnerabilities or whatever. Can we and should we kind of focus this definition a little more tightly?

Ms. ROAT. Yes, sir. We should take a look at that to make sure that we're aligned on the definitions and that we're all speaking on the same page as we're looking at the definitions of programs across the Federal Government. I mentioned three with three definitions on that, where, you know, GAO is using the high-priority programs and some of the other ones. So, I agree with you, we should take a look at that and make sure that we're all in alignment.

Mr. HICE. OK. I agree. Let's try to move forward on that.

Also, another thing that has come up, when it comes to legacy IT, the current scorecard does capture whether or not an agency has a working capital fund, but it does not deal with whether or not any of those funds are being used to modernize old systems.

So, my question really is, what kind of metrics can we add to the scorecard to incentivize agencies to make these kind of IT overhauls that need to be made? We've got to make the transition.

Ms. ROAT. I agree with you. It is imperative that we continue to modernize. The IT working capital fund is one of those programs that allows agencies to have that long-term sustained investment in technology that is incredibly—that's critical to modernizing. So, the IT working capital fund, where you can have multi-year dollars

within those, that's the intent, is to modernize those legacy systems and really drive that modernization over multiple years.

Where you have legacy systems and programs, being able to invest that over multiple years is the way you get out of, you know, that technical debt and you continue to move the ball forward on that. So, with the Technology Modernization Fund and the IT working capital fund, those are two critical programs for agencies to sustain long-term modernization.

Mr. HICE. OK. Thank you.

My last question will kind of deal with the customer service aspect. More and more we're having people who are involved in coming to the government digitally. What about, how can we put this type of metric in future scorecards to make sure that we are providing the customers what they need?

Ms. ROAT. Thank you for that. There's—with the IDEA Act, I think there's an opportunity to really look at the customer experience. That was the intent of the 21st Century IDEA Act—the customer experience and how they interact with the Federal Government. And there's a number of requirements in there, from e-signatures to 508 to enabling an easier customer experience with the Federal Government.

So, I look forward to working with you and the committee on understanding what are some good metrics on that, because that is a perfect example of a metric that could evolve over time as agencies are continuing to improve their websites and their customer experience with the American public.

Mr. HICE. Thank you very much. I yield back.

Mr. CONNOLLY. I thank the gentleman.

And that's a good point, Ms. Roat. We'll be glad to work with you on that.

Before I call on Mr. Lynch for his five minutes of questioning, Ms. Harris, did you want to address the question Mr. Hice raised about what falls under the penumbra of high risk on the scorecard?

Ms. HARRIS. Sure. So, high risk is defined by each of the individual agencies. So, it could be cost, a certain cost threshold. It could be a high-value asset. There are a number of ways that agencies do define what they consider to be high risk.

And I think that having—I think OMB would play an excellent role in having a more uniform decision or even having perhaps a watch list of the 10 to 20 top critical IT investments across the government would be an excellent way to be able to focus and hone down what those high-risk investments are. We have work for this committee, looking at the top 10 to 20 mission-critical IT acquisitions across the government where we have put together the list for you. That report will be coming out in September. We would be happy to work with OMB to perhaps use that list as a jumping-off point to have another working list for OMB and the executive branch agencies to work from.

Mr. CONNOLLY. I would just say a word of caution. When we began this category, there were agencies that claimed they had no high-risk projects, none. No, everything is fine, nothing to look at here. We needed to get out of that protective defensive mode, candidly, to say, hey, these are high risk for these reasons and we're

going to monitor them so that they don't go awry, but if they do, we'll take quick action.

Because that was part of the problem FITARA was trying to address, that we had these long multi-year, multi-billion-dollar systems integration projects, and nobody felt empowered to pull the plug if the milestones weren't being met. In fact, there weren't always milestones. And we were trying to make sure that we didn't make a bad thing worse.

In the private sector, if something goes awry, the CEO says, pull the plug, we're going to move on, we'll try something different. A little harder to do in the public sector, because everybody wants to know why did you waste the money? But nothing is improved by doubling down on something that's not working.

So, high risk really matters and getting it right really matters, and we don't want unwittingly to change the definition so that we go back to the old days of everything's fine, because the point isn't to ding on people because it's bad, it is to capture something going awry before it goes off the cliff.

But I thank you, Mr. Hice, for raising it, because I think some uniformity of understanding probably would be a good thing.

Mr. Lynch, I'm sorry to impose on your time. Welcome.

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

I want to followup on that sentiment, because you and I know, as longtime members of this committee, that, you know, it's been a history of we don't have any problems over here, we're good, until there's a blowup like we had at OPM when 22 million records went out of people who were applying for security clearance and others that were in government as well. So, we saw the disasters. So, I approach this with a little bit of skepticism, just healthy skepticism. I'm happy to hear the good reports, don't get me wrong, but I've been here too long to believe all of that.

So, I want to ask about—you know, let's go to Mr. Gray. You know, I read recently a pretty good story in The Washington Post that talked about thousands and thousands of borrowers of student loans whose personal information, their Social Security numbers, their detailed financial information was left exposed by the Department of Education for like six months. And it had all their personal—you know, these were people looking for some relief. Either they had been taken advantage of or exploited by for-profit universities, those type of cases. So, they had to basically open the kimono of these applicants who were looking for relief, and yet we left all their information available to whoever would tap into it. So, that's one issue I got. I'd like to hear from Mr. Gray on that.

Then on OPM, I noticed the grade is a C. And given the, you know, history here—and we all know what it is, I mean, just horrific, horrific, and OPM had not even encrypted Social Security numbers. It was just an unmitigated disaster, and we continue to suffer from that today because of all the people we exposed who had asked for security clearance, right? Those are the people that do some of the most sensitive work in our government, and they were all exposed because of the lack of cybersecurity at OPM.

So, I'd like to hear from Mr. Gray and also someone who can speak on behalf of OPM as to why they only have a C at this point. Thank you.

Mr. CONNOLLY. We'll ask Mr. Gray to go first, and then we'll call on Ms. Martorana.

Mr. GRAY. So, thank you for that question. I will share that that article is incorrect. The Department did not leave that open for many months. What really happened was that we had a situation where a file share was inadvertently left open to internal Department only employees. As this was briefed on Friday, there was no external access. It was not open. It was one element. We did report, as required, through OMB Memo 20–04.

It is a low-risk incident. And as I briefed this committee on Friday, it is a situation like being in a bank where a bank has a vault. Every employee that can go into that vault is a trusted employee. Every person that works at the Department is vetted. They have fingerprints. They have user agreements. They have annual cybersecurity and privacy awareness training, records management training.

This is a situation where an employee actually recognized that a safety deposit box in that vault that external people could not get to was unlocked. It should not have been unlocked.

Mr. LYNCH. Mr. Gray, hold on for a second.

So, did every single person have a need to know in each of those cases, or was it looser than that?

Mr. GRAY. Every employee is vetted to be able to access information and, no, not every employee needed to access that. And as of this morning——

Mr. LYNCH. OK. That's all. You need to tighten that up. So, you need to tighten that up, right?

Mr. GRAY. Absolutely, and we absolutely did.

Mr. LYNCH. It's not exactly what the Post led me to believe, but we can tighten it up, right?

Mr. GRAY. Yes, Congressman, we can, and we have.

Mr. LYNCH. OK. So, let me go—I only have a minute left, so let me go to Ms. Martorana on OPM, please.

Mr. CONNOLLY. You need to turn on—thank you.

Ms. MARTORANA. Sorry. Thank you for the question.

We continue to work diligently at OPM to upgrade our infrastructure, upgrade our overall cyber posture. We are struggling with our staffing. We are struggling to make sure that we have appropriate staff levels to support all of the systems that we are maintaining.

One of the biggest challenges that we do have is we are still supporting our Department of Defense colleagues as we are decoupling our systems. So, we are still, on a daily basis, operating DCSA, the national background investigation systems, on all of their daily operations, as well as all of the laptops and their desktop support services, et cetera.

So, as we are able to hand that mission fully over to the Department of Defense and focus singularly on OPM, that will give us the opportunity to be able to focus on OPM's core mission and upgrade all of the services that we deliver to our own mission.

Mr. LYNCH. OK. That's a fair answer.

Thank you, Mr. Chairman, for your indulgence. I really appreciate the courtesy. Thank you.

Mr. CONNOLLY. Mr. Lynch, if I could followup on that question, I understand the sequencing with the Department of Defense; but when we go back to the original breach, and you weren't there, part of the problem was that we had software for cyber protection, Einstein, and there was Einstein 2 which had not been installed. Now, that has nothing to do with the Defense Department.

That's a management issue about getting around to it, prioritizing. I wonder if you want to take a moment to try and reassure Mr. Lynch and the rest of the subcommittee that that attitude has changed, that, in fact, we are prioritizing cyber and protecting our data bases at OPM.

Ms. MARTORANA. Yes. I can assure you that the rigor and discipline within the current OPM team is extraordinary. We would not have been able to execute something as complex as our main frame migration without having a disciplined management team and extraordinary CIO team that is doing a diligent job on a daily basis.

Can we do better? We can always do better, right? IT is one of those areas where you can always improve; but the team is extraordinary, and we work utilizing every single tool and asset available to us.

Our cyber team and our CISO are extraordinary, and we do everything possible to safeguard every single asset within our environment. We utilize the best tools of the Federal Government, including DHS, to support us, the perimeter of OPM. So, I think you can rest assured that at this time all safeguards and standards are being operated at the highest level.

Mr. CONNOLLY. Thank you.

And thank you, Mr. Lynch.

The Chair now recognizes——

Mr. LYNCH. Mr. Chairman, thank you.

Mr. CONNOLLY. Thank you.

The Chair now recognizes our returning colleague, the gentleman from Alabama, Mr. Palmer, for five minutes.

Mr. Palmer?

Mr. PALMER. Can you hear me now?

Mr. CONNOLLY. Yes, sir, we can. We can't—is your video on, Mr. Palmer?

There you are.

Mr. PALMER. It is.

Mr. CONNOLLY. There you are.

Mr. PALMER. You got me? All right.

Well, first of all, I want to compliment Mr. Lynch on his library. That's impressive.

Mr. CONNOLLY. I hear he rents it.

Mr. PALMER. He rents it.

Ms. Harris, there was a 2018 report submitted before the U.S. China Economic Security Review Commission that found that the Federal Government's top seven IT providers sourced over 51 percent of its materials from China since 2012. And I just want to ask you if you think that this poses a significant economic and national security risk.

Ms. HARRIS. Yes, sir. This is significant, a significant risk to national security. We had work ongoing for this committee related to

the IT cyber supply chain, and the vast majority of the agencies have not instituted proper supply chain internal controls. This is a major issue. We're going to be making more than a hundred recommendations associated with this. But it does pose a significant threat to our Nation.

Mr. PALMER. Well, and I bring this up, Mr. Lynch raised the question about the breach at OPM, that I think there are still issues with that, with that information, the personal identification information that's still out there.

What would be the budgetary impacts of shifting Federal technology acquisitions away from China?

Ms. HARRIS. Sir, I'm not in a position to answer that question. We have not done work specific to that, unfortunately, so I'm not in a position to answer that with specific facts.

Mr. PALMER. Ms. Roat, would you at OMB have an idea about that?

Ms. ROAT. No, sir, I do not.

Mr. PALMER. Well, I think that's something that we need to get an estimate on. I think we're talking—there's a tremendous amount of talk about shifting the supply chain out of China, particularly when it comes to drugs and materials that are critical to our economy and to our national defense.

And the fact that—I think, Ms. Harris, you're the one a few minutes ago that said that we spend 80 percent of our budget on maintaining antiquated systems. Is that correct?

Ms. HARRIS. Yes, that's correct.

Mr. PALMER. And then 51 percent of that is sourced from China, I think. So, I think this is something—and I'm going to make this request to Ms. Roat and to Ms. Harris that either your agencies come up with the estimate or you work together to come up with that estimate—if I need to, Mr. Chairman, I'll put that in writing; but I think we need to know what it would cost us to shift our IT supply chain away from China.

So, I would appreciate it if we could get a response from you and let us know when you start working on it.

The Commission also recommended Congress to establish a comprehensive national security supply chain management strategy. It further recommended that direct statistical agencies, such as the Census Bureau, review methodologies for collecting and publishing deeply detailed supply chain data to better document the country of origin for imported goods from China, including imports related to our Federal IT system.

And this is for all of the witnesses. Are you aware, are any of you aware of any current actions that the Federal Government is taking to implement these recommendations?

Ms. Harris, let's start with you.

Ms. HARRIS. Sir, I don't—that work is out of the scope of what I am doing for this committee. So, I'll have to take that for the record to see if there's a better expert within GAO to answer that for you.

Mr. PALMER. OK. Mr. Gray? Well, that would be outside of your area of expertise, too.

I'll go to Ms. Roat. Do you know where we are on that?

Ms. ROAT. Right now we are working very closely with agencies to take a look at their supply chain, currently briefing them out on the requirements of section 889, but, again, working very closely with the agencies to understand their footprint and what the impacts are on that. So, that work is ongoing and will continue.

Mr. PALMER. Is it specific? Are there specific—is there specific work being done on the IT systems?

Ms. ROAT. Again, we're working with the agencies to understand, as you alluded to, what the impact is and understanding if there's equipment that needs to be replaced, upgraded, those kinds of things, the impacts on those systems. So, that work, we have kicked it off and that is underway right now.

Mr. PALMER. OK. I thank the Chairman, and I yield back.

Mr. CONNOLLY. Let me just say to the gentleman, I think he raises a really good point about the need for coordination so that we're not, you know, retiring legacy systems with 150 different systems that can't coordinate, or can't be encrypted, or have different requirements as much as we can in coordination by OMB to make sure—and the CIO and CTO in the White House to make sure that we're making prudent decisions for the future, both in the cyber realm and in terms of interoperability and coordination, very important.

Mr. PALMER. Mr. Chairman, if I might respond to that?

Mr. CONNOLLY. Thank you, Mr. Palmer.

The Chair now recognizes——

Mr. PALMER. Mr. Chairman, if I may respond to that?

Mr. CONNOLLY. Of course.

Mr. PALMER. May I respond to that?

Mr. CONNOLLY. Yes, you may.

Mr. PALMER. You're absolutely right about the interoperability among Federal agencies, but it also should extend to the states, and we're seeing—in my previous experience on the Oversight Committee, we saw multiple examples of the inability because of the antiquated systems to have that interoperability between state agencies and the Federal agencies.

I just wanted to add that. And I yield back.

Mr. CONNOLLY. You are quite correct, and we're certainly seeing that in unemployment IT systems all across the country. There are at least a dozen that still use COBOL. Now, the only good news about that is I understand that the Chinese don't know how to hack into COBOL, but that's about the only good news.

So, you're absolutely right, and we're seeing that affect millions of Americans in terms of not getting their payments in a timely fashion, which creates a snowballing effect in their ability to cope during the pandemic.

The Chair now recognizes the gentleman from Maryland, Mr. Raskin, for his five minutes.

Mr. Raskin?

Mr. RASKIN. Yes, Mr. Chairman.

Mr. CONNOLLY. Welcome.

Mr. RASKIN. Thank you very much. I'm sorry, I thought I was unmuted already.

Mr. CONNOLLY. No problem.

Mr. RASKIN. Thanks for calling this very important hearing.

In June of last year, the day before the FITARA 8.0 hearing, OMB issued guidance which revised and narrowed the definition of a data center. According to GAO, this revised guidance eliminated reporting on more than 2,000 facilities governmentwide, including types of facilities that OMB had previously cited as cybersecurity risks.

Removing the requirement to report on these facilities diminishes our ability to exercise oversight over potential security risks. Ms. Harris also noted in her opening statement that consolidation of data centers has saved us billions in taxpayer dollars. So, why would we discontinue efforts that save money and improve cybersecurity?

Ms. Harris, does GAO remain concerned with OMB's decision to change the definition of data center and to no longer require agencies to include smaller data centers in their data center inventories?

Ms. HARRIS. Yes, sir, we still remain very concerned about the new definition of data centers. Our concern in particular is because when agencies stop reporting on these data centers, they'll fall under the radar. They'll stop looking at them in general, and then that's where the cybersecurity vulnerability risks increase because they're not looking and paying attention to these centers.

Mr. RASKIN. Yes. And OMB's changes to the new guidance no longer allowed the subcommittee and GAO to evaluate agency progress toward data center optimization and consolidation.

Ms. Roat, can you tell us why OMB would stringently narrow the definition of data center when doing so could both impair cybersecurity and increase costs to the taxpayer?

Ms. ROAT. Thank you for the question.

So, OMB updated the definitions of data centers to better align with industry standards. When you look at the overall definitions of data centers, those areas where there was maybe just a router and a switch in a closet somewhere, those really aren't classified as true data centers because they have com gear in it. So, those types of things were changed as part of the definition.

As you look at the modernization across the Federal Government and agencies closing data centers, they are taking big steps to rationalize their portfolio, upgrade their infrastructure, and address those cyber security concerns just across the entire environment.

So, as you shut down data centers, there are many steps behind it to do that. So, even as we change the definition of data centers, modernizing and closing and shutting down data centers per the industry standards takes a lot of work and those application, rationalization and infrastructure upgrades will continue as we close data centers.

Mr. RASKIN. Well, will you commit to working with the subcommittee to track data centers in ways that are consistent with the law and GAO's recommendations to improve cybersecurity and maximize the saving of tax dollars?

Ms. ROAT. Yes, sir. We look forward to working with the committee on those data center metrics.

Mr. RASKIN. OK. Agencies required to implement the data center consolidation reported in total $4.7 billion in cost savings from Fiscal Year 2012 through 2019. Of these 24 agencies, 23 reported in

August of last year that they had met or planned to meet OMB's Fiscal Year 2019 savings goal of $241.5 million.

Ms. Roat, do we now know whether agencies met their Fiscal Year 2019 cost savings goals? If not, when will we have that knowledge?

Ms. ROAT. I'll work with OMB on those data centers and those metrics to make sure that we have accurate information for that, but we continue to track what the agencies are reporting to make sure that progress continues on the cost center and savings.

Mr. RASKIN. OK. Thank you for that.

Ms. Harris, is there any more potential for cost savings through data center consolidation?

Ms. HARRIS. Yes. We believe that there is, and so that is why this should continue to stay as a priority for the committee on the scorecard, as well as for the agencies.

Mr. RASKIN. Well, why has the Administration chosen to halt its efforts in this field?

Ms. HARRIS. Unfortunately, I don't feel comfortable speculating as to why the OMB would make that decision; but, again, you know, backtracking on identifying and including things like servers in closets and considering that to be a data center is something that we disagree with OMB on.

That is something that should be counted because it may not be an opportunity for consolidation, but it certainly still poses a threat from a cybersecurity standpoint. So, we do believe that having the more inclusive definition is the way to go.

Mr. RASKIN. OK. Can you describe the barriers to cloud adoption in your approach to removing those barriers?

Ms. HARRIS. Well, the barriers to cloud would—it would be—the No. 1 barrier is agencies having it as a priority. We've found in our work on cloud adoption that agencies don't necessarily have the robust processing in place to take a look at all of the investments that they have in terms of whether or not they would be eligible candidates for the cloud.

So, we've made recommendations to the agencies in implementing those processes, and we currently have work to look at whether those agencies are in the process of implementing the recommendations that we've made to them.

Mr. RASKIN. OK. I think I have run out of time, Mr. Chairman. Thank you very much for your indulgence.

Mr. CONNOLLY. Thank you very much, Mr. Raskin. And your point about data center consolidation is very important, and I agree with you.

Let me just say, Ms. Roat, I wrote that section of the bill, so I care about it, and I'm not going anywhere.

So, we are going to insist on a robust definition of data centers so that we continue the goal of consolidation to, A, effectuate savings that can then be used internally for reinvestment because they are one of the big sources of potential savings and, second, in the whole mission of cyber protection.

So, we'll work with you, but we're not going to countenance squishiness in the definition so that people get off the hook and aren't accountable for what were the data centers we're trying to consolidate. So, I hope you will take that message back.

The gentleman from Wisconsin, Mr. Grothman, is recognized for five minutes.

Mr. GROTHMAN. OK. Do you see me on there?

Mr. CONNOLLY. We can hear you. We can't yet see you.

Mr. GROTHMAN. Well, you might have to put up with just hearing me. Oh, there I am.

Mr. CONNOLLY. There you are.

Mr. GROTHMAN. OK. I got in a little bit late.

Is Ms. Martorana still around?

Mr. CONNOLLY. Yes, she is right here.

Mr. GROTHMAN. Good, good, good, good, good, good. OK.

I understand you spent a lot of your career in the private sector and are focused on improving the digital experience. Given OPM's importance to the Federal work force and public, could you describe how you approach digital modernization?

Ms. MARTORANA. Sure. There's an enormous opportunity for us at OPM to better serve our customers across a broad spectrum, from continuing to improve the opportunity for job seekers all the way through to retirees.

So, there are numerous opportunities. But the most important place to start is on a firm platform and starting with the foundational investments that are required in people and technology to start that digital modernization journey.

Mr. GROTHMAN. OK. I'll ask you another question together with Jason.

[Inaudible] Ms. Martorana, and what steps are you taking to comply with FISMA—[inaudible]

Mr. CONNOLLY. Mr. Grothman?

Mr. GROTHMAN. Yes.

Mr. CONNOLLY. I'm sorry, could you repeat your question? It sounds like you're in a railroad train.

Mr. GROTHMAN. OK. I'm sorry. I'll speak up.

Mr. CONNOLLY. That's OK.

Mr. GROTHMAN. OK. Both of your agencies—this is both for Ms. Martorana and Jason Gray. Both of your agencies have critical missions and process sensitive data, yet both of your agencies get C's in cybersecurity, which means you have got room for improvement.

What steps are you taking to comply with FISMA, a critical tool for ensuring effective information security across the government?

Mr. GRAY. So, I will start. We have taken a four-phased approach, focusing on our processes and making sure that we're refining our processes to not only comply with FISMA but also enhance our cybersecurity posture.

We're also looking and have been focused on strengthening our processes as it relates. We also have a lot of tools that we have and continue to use with defense in depth, a whole bunch of them.

Then also equally as importantly, as was mentioned earlier, education. So, it's focusing on making sure that our staff understand that and the department as a whole understands the importance of cybersecurity.

We've also developed and implemented a cyber risk scorecard that we produce that has near real-time metrics that shows it's aligned directly within the cybersecurity framework, and that is

visible to our system owners so they can see exactly how they're doing.

To the comment earlier about making sure that we're measuring the risk and actually when something is red, it's not necessarily a bad thing. It's an indication that that needs some work. That gets briefed every single month to the secretary, the deputy secretary and monthly to all of the assistant secretaries for all of theirs.

So, it is really focused on a process improvement, policy improvement, leveraging the tools that we have, and making sure that we're educating everyone at the department on the role of cybersecurity.

Mr. GROTHMAN. OK.

Ms. Martorana, do you have anything?

Ms. MARTORANA. Yes. And I think I can mimic basically. We are probably a little bit behind where the Department of Education is, but following in those footsteps, the people, the process, adding new technology and tools, and significant training. We are consistently training our work force to make sure that the policies and processes that we develop and the tools that we are implementing are understandable and that the entire work force is comprehending that every single one of us are the best tools that we have in keeping all of our information systems safe and secure.

Mr. CONNOLLY. Mr. Grothman?

I think that train left the station.

OK. Thank you, Mr. Grothman.

The Chair will now recognize himself for his five minutes of questioning.

Oh, you're back? Glenn, did you have one more question?

Mr. GROTHMAN. Yes, yes.

Mr. CONNOLLY. Go ahead.

Mr. GROTHMAN. Ms. Harris, at this point nearly all agencies have gotten A's in the software licensing metric. Do you think it's time to remove this metric? And, if so, how can we evolve this metric to capture some of the cost saving aspects like eliminating unused software licenses?

Ms. HARRIS. Yes, that's a great question.

So, I think that given all agencies except OPM have received that A, it may be time to retire that particular metric or evolve it. Certainly when it comes to the evolution of the metric, one of the key things that we'll have to work with with this committee on, as well as with OMB, is the availability of governmentwide data that's publicly available because that's what is used in order to generate all of these scores or these grades.

So, that would be a key factor in what we could use to potentially evolve the software licensing grade.

Mr. GROTHMAN. Thanks much.

Great hearing and thanks for putting this together.

Mr. CONNOLLY. Thank you, Mr. Grothman. Thank you for joining us.

Ms. Harris, despite all of the progress in the scorecard, we really don't seem to have made progress in retiring legacy systems. Why not? And what will it take to seriously incentivize agencies to do that?

Ms. HARRIS. Mr. Chairman, I think what we need to see greater progress on is the working capital fund establishments because that's a very important mechanism that the agencies can use to transform their IT and to modernize it.

So, we would like to see a more aggressive push by the agencies that have not yet implemented those working capital funds to do so as quickly as possible so that they're able to put those savings that they generate from software licensing, from portfolios and data center consolidation into that fund so that they can use those moneys to be able to—and the flexibilities associated with a working capital fund, to be able to modernize their platforms.

Mr. CONNOLLY. Mr. Gray, you will forgive me, but I think you soft pedaled the breach.

So, yes, the breach may not have been huge but, you know, this committee had a hearing on your agency or including your agency several years ago, and what came out was surprisingly, although maybe not surprisingly, but the Department of Education actually has a huge data base, 40 million Americans. You applied for a student loan, you've got my financial data, my checking account, my savings account, all kinds of other financial data that's pretty sensitive. And that's a pretty big data base and a juicy target for some people up to no good.

So, the fact that we had this breach raises the question about how secure is that data—the bigger data base. And given the fact that you get a C minus in cyber, one of your lower grades, it underscores vulnerability, maybe I need to be concerned. I wanted to give you an opportunity to talk about that.

Mr. GRAY. So, I appreciate the question. The incident that happened in 2017 is obviously very different than what happened here. What was briefed on Friday is that we literally had a file share, one out of over 7 million folders, one where a user inadvertently allowed other people within the department permissions.

If you have a situation where people have the ability to go through and say, hey, I'm going to allow people to have access to this, that sort of thing will happen.

In this situation the employee who actually identified that did not report it to the department. They reported it externally to the department. To compare this to the TSA, this would be like a TSA individual at an airport seeing a suspicious package and instead of reporting it, seeing something, saying something, they took it externally, which then went to the media.

So, to get to your question, though, I agree this was identified. When we were reported—when it was notified to me, we took care of it right away. We've also gone through and scrubbed and rescrubbed. We've hired a third party to come in and recheck all of what we've done just to make sure.

As of this morning, they have come to the same exact conclusion as it relates specifically to this incident. This is a low-risk incident where an internal—as I mentioned about the bank and the safety deposit box, it was for trusted employees. In this case we had a trusted employee who saw something and instead of doing what they were supposed to do, they took it external.

To get to your question about cybersecurity, absolutely I take cybersecurity seriously. I have been at the department for over four

years. This is my fifth agency that I have been at. Cybersecurity is certainly one of the core focus areas that I have had. We, as I mentioned, have gone through what processes can we improve, is there policies that we need to implement, are there additional tools which we—as I mentioned, we have network access control, data loss prevention. So, we're taking a lot of necessary steps to ensure that we're protecting and defending the information that we are entrusted to.

Mr. CONNOLLY. You have legacy systems at the Department of Education?

Mr. GRAY. Yes one.

Mr. CONNOLLY. One. How old is that system?

Mr. GRAY. I would have to get you an exact number, but it's probably been around longer than I have.

Mr. CONNOLLY. Wow. Well, I have two conclusions from that. One is you're younger than I thought or the other is ah, gosh, you know, that really puts an exclamation point on it.

From your point of view, and you have had experience in other agencies, let's stipulate we need a working capital fund. But other than that, what's it going to take? Because my experience is, in the private sector, management needs to put a priority on something if it's going to happen. There has to be a multi-year commitment if that's what it takes. You've got to back it up with a budget commitment every year.

From your point of view, what's it going to take to retire that legacy system?

Mr. GRAY. To continue on the path that we're on—actually there's a Next Gen financial student aid system that is well underway. That acquisition or that entire group of projects incorporates removing that legacy system and getting rid of it. So, it is actually on the road map on where we're going.

General Mark Brown, who leads the Federal student aid, has been doing an amazing job working very closely—both of our teams working closely together from an oversight standpoint, to make sure that we are—it's fed into our governance process.

So, at this point we have the support. Funding is always something we can always use, but we have the absolute support from the Secretary, from leadership and governance to address that legacy system because we do recognize it is old and needs to be improved.

Mr. CONNOLLY. It is an enormous opportunity cost, not only for you but the rest of the Federal Government. If we're spending 80 percent of a $96 billion line item—well, it's not a line item, but that's roughly our budget for IT every year, and 80 percent of it is going just to maintain legacy systems, no wonder we've got some of the problems we've got.

So, Ms. Martorana, you're relatively new to OPM. Where did you come from, may I ask?

Ms. MARTORANA. The United States Digital Service. I spent two years at the Department of Veteran Affairs prior to joining.

Mr. CONNOLLY. OK. And you had private sector experience before that?

Ms. MARTORANA. Yes.

Mr. CONNOLLY. OPM got, I think, a C, C minus overall grade.

Given the fact that you're the H.R. agency for the entire Federal Government and, as Mr. Lynch mentioned, really sensitive data on Federal employees, on people seeking security clearances, you know, a breach there, what could go wrong with that? And, sadly, we had the biggest single breach in the history of the Federal Government with your agency several years ago.

There is a sense, not about you personally, but that the agency remains surprisingly less than driven by a mission to make sure that never happens again and we're the exemplar for the Federal Government as opposed to a laggard. So, I want to give you the opportunity to address that. I heard you like your team and they're committed and you feel pretty good about where you're headed, but a C minus is not a great overall grade for—given your mission. And maybe put more positively, as we look to the future, what will it take to get to an A from your point of view.

Ms. MARTORANA. Yes. We're a C plus, so a slight correction.

Mr. CONNOLLY. What's that?

Ms. MARTORANA. C plus.

Mr. CONNOLLY. C plus rather; excuse me.

Ms. MARTORANA. With the mainframe platform migration that we just completed and the coming data center closures that that will trigger and the—we had a failing grade in software inventory, but through the COVID supplemental, we're able to procure software that will allow us to actually do a software inventory. We will be able to check that off of our list as well, which should get us to approximately a B FITARA score within the next six months. So, we are making pretty significant progress.

You know, security is our primary focus, right. Every single day we keep those systems safe, secure, and operational. But one of the biggest challenges that we have is funding and personnel. To the question earlier about risk, one of the biggest risks I think that we are facing, in addition to those systems, the legacy systems, is also we have many, many people in our work force that are retiring.

And with those folks retiring and a lot of these systems' documentation not—systems being old and not being very properly documented, a lot of the knowledge of those very old complex legacy systems is retiring with those subject matter experts.

So, I think we have multiple levels of challenges that we have to face together. So funding, multi-year funding so that we can actually retire those legacy systems and put in more modern technology, that will reduce risk.

Continuing to upskill and train our Federal work force and inspire younger and different people to come into the Federal work force is a critical part of what is going to be needed for us to continue to secure and maintain and operate those systems.

Mr. CONNOLLY. I certainly agree with you, although I would say, not about you, you know, freezing wages, threatening to cut back in compensation, disparaging the work of the Federal work force, making it harder for people in the workplace to have appeals and representation and talking about extending a probationary period from one to two years, none of that is particularly appealing to young people on the college campus to come work for the Federal Government.

It's almost designed, in fact, to also accelerate the phenomenon of retirement when people—40 percent of the Federal work force is eligible for retirement, and some of them can delay it because they're so driven with their mission and so passionate about what they're doing, or they can accelerate it because they feel so discouraged and unappreciated. And none of this was helped by a 35-day shutdown, the longest in American history.

So, you come from the private sector; I come from the private sector. I don't know a CEO who would get very far with his or her board disparaging the work force, slashing compensation and talking about—you know, discrediting, shall I say, their value and their work. No CEO I know would keep the job.

And, you know, you praise your work force, you motivate your work force, you incentivize your work force——

Mr. PALMER. It looks we lost the Chairman. Is he still on your screens?

Mr. CONNOLLY. OK. Well, anyway, I want to thank you for the observation. Thank you for the work you have done. We will stay in touch. Congratulations on progress.

And we certainly, Ms. Roat, need OMB to keep the pressure on and to be supportive. We've got to come up with some creative solutions to help agencies, in addition to money, retire these legacy systems. And they want to, they're motivated, but it's a big, big decision and a multi-year commitment in most cases and quite disruptive actually in making that transition.

So, we've got to have some creative solutions. As we see the vulnerabilities in our systems, they have to be addressed.

Thank you to the first panel so much for being here today. Please stay safe and healthy.

We're going to take a five-minute break and then convene the second and final panel of this hearing.

Thank you.

[Recess.]

Mr. CONNOLLY. The subcommittee will reconvene.

Mr. Powner, Ms. Council, and Mr. Spires, are you with us?

Mr. Powner, can you unmute and acknowledge you're with us?

Mr. POWNER. Yes, I'm here, Mr. Chairman.

Mr. CONNOLLY. Thank you. If you would stay unmuted so I can swear you in.

Ms. Council, are you with us?

Ms. COUNCIL. Yes, Chairman Connolly.

Mr. CONNOLLY. Thank you.

And, Mr. Spires?

Mr. SPIRES. Yes, Chairman Connolly.

Mr. CONNOLLY. Thank you.

If all three of you would raise your right hand. Do you swear to tell the truth, the whole truth and nothing but the truth or affirm the same, so help you God?

Let the record show all three of our witnesses on the second panel have affirmed in the positive.

Thank you.

Mr. Powner, if you're ready, I'm going to call on you for your five-minute opening statement.

And welcome back to our subcommittee.

Mr. POWNER. Thank you.

Mr. PALMER. It's good to be back, Mr. Chairman. I don't have an opening statement.

Mr. CONNOLLY. I would ask—oh, Mr. Palmer?

Mr. PALMER. Yes, sir.

Mr. CONNOLLY. I'm sorry, I didn't see you. Go ahead.

Mr. PALMER. OK. I do not have an opening statement, but I failed to do something in the previous panel, and that is enter a document and ask for unanimous consent to enter a document into the record on the supply chains vulnerabilities.

Mr. CONNOLLY. Certainly, yes.

Mr. CONNOLLY. And, Mr. Palmer, if you didn't hear me, I said I would be glad to work with you on that whole question about supply chain. I think it's a very good point you made.

Mr. PALMER. Well, I had hit the little raise my hand button thing—I'm trying to get used to all of this webinar stuff—and I had a followup question that I will ask one of the panelists here.

But with that, with no opening statement, I will yield back so that we can move forward with the questions for the panel.

Mr. CONNOLLY. Thank you, Mr. Palmer. I didn't call on you for an opening statement because Mr. Hice had an opening statement for the whole hearing, and this is the second panel of that hearing. But, obviously, if you had something you wanted to add, you're more than welcome.

Mr. PALMER. I thought you were asking me if I had an opening statement. I do not, but I will have questions.

Mr. CONNOLLY. Yes, of course, and we welcome them. Thank you.

Mr. PALMER. And I thank the Chairman.

Mr. CONNOLLY. Mr. Powner, you're recognized for your five minutes.

STATEMENT OF DAVID POWNER, DIRECTOR OF STRATEGIC ENGAGEMENT AND PARTNERSHIPS, THE MITRE CORPORATION

Mr. POWNER. Chairman Connolly, Ranking Member Hice, and Members of the Subcommittee. Thank you for the opportunity to testify on the FITARA scorecard.

For the past two years, I have worked for MITRE, a not-for-profit corporation that operates in the public interest. We're public/private partnerships with federally funded R&D centers. We work across government, partnership with industries to tackle challenges for the safety, stability, and well-being of our Nation.

Prior to joining MITRE, I was at GAO where I worked closely with this committee crafting FITARA, helping with the creation of the scorecard, and assisting in its oversight.

I would like to start by thanking you, Chairman Connolly, for your leadership not only in creating FITARA, but also your unprecedented follow-through with more than five years of consistent oversight which has included 10 scorecards.

The Federal IT community has benefited greatly from working with you and your bipartisan partners along the way, Representatives Issa, Hurd, Kelly, Meadows, and now Ranking Member Hice.

Today I would like to address three areas: One, the results and progress that have occurred since FITARA passed; two, the reasons

for these results; and, three, potential areas to consider for future scorecards.

The progress that has resulted from the scorecard in your oversight are significant. Billions of taxpayers' dollars saved consolidating data centers and reducing duplicative business systems and licenses. FITARA's scorecard has also helped elevate the CIO role. More CIOs have a seat at the executive table and relationships with agency CFOs have strengthened. These enhanced authorities and relationships will be critical as CIOs lead their agencies to more modernization and digital transformation.

So, why was FITARA and its implementation successful? Simply put, it was a collective team effort from the Legislative and executive branches. Let's look into the specifics of this oversight. Mr. Chairman, your approach focused on critical sections of the law, established clear metrics with specific targets, was measurable and data driven, and the oversight was consistent every six months over a five-year period. This is extremely important since it took at least two years with four scorecards to see significant progress in any of the graded areas.

Also, OMB played a critical role. They issued FITARA implementation guidance and required self-assessments after FITARA was passed. Federal agencies' CIOs have provided leadership and delivered results. This progress is evident with the high grades on today's scorecard.

So, where should the scorecard go from here? Some of the areas graded have reached a level of maturity where perhaps grading is no longer a necessity. Now, this is not to say that they're not important, just that other areas could benefit from the transparency, measurement, and oversight the scorecard provided.

For example, Mr. Chairman, the hearing you held a few weeks ago on mission modernization and your March hearing where you covered GSA's EIS contracting are prime candidates.

My written statement provides five recommendations to consider as the scorecard is enhanced. These recommendations are very consistent with the goals in the President's management agenda. Here's a brief rundown of the five.

No. 1, enhance the cyber area by considering metrics with agency and industry use and measure cybersecurity. This should include areas like patch and vulnerability management, missed cybersecurity framework, and supply chain management.

No. 2, add a mission modernization category that provides transparency to our Nation's most important IT acquisitions and incorporates a customer experience measurement as well as legacy retirements.

No. 3, add an infrastructure category that highlights progress on EIS so that we have in place more modern and secure networks.

No. 4, add an IT work force category that provides a comprehensive view of agencie's gaps in critical cyber engineering areas and tracks progress to build the appropriately skilled work force.

And, No. 5, add an IT budgeting category that continues to focus on working capital funds but also incorporates TBM so that IT costs are better captured.

We need to shed a light on the discipline agencies use in IT budgeting so that it reflects actual needs for modernization. This

category could drive better conversations both internally with CFOs and externally with OMB and the Congress.

In summary, Mr. Chairman, these recs are about having better secure agencies, tackling true mission enhancement, having a modern infrastructure, a skilled work force to do it, and the right resources.

Could an enhanced scorecard help in these critical areas? Absolutely. Future legislation to enhance OMB policies could also.

Mr. Chairman and Ranking Member Hice, we look forward to further assisting you on these important topics for our Nation.

Mr. CONNOLLY. I thank you, Mr. Powner, and I also thank you for being one of the architects, key architects of establishing the scorecard, and I think it's evolved in a way that we hoped it would, which is to incentivize agencies to evolve and to modernize and to understand the criticality of that mission. And I thank you for your leadership in allowing us to be where we are five years later.

LaVerne Council, chief executive officer of Emerald One, welcome.

STATEMENT OF LAVERNE COUNCIL, CHIEF EXECUTIVE OFFICER, EMERALD ONE, LLC

Ms. COUNCIL. Chairman Connolly, Ranking Member Hice and Members of the Committee, thank you for the opportunity to appear before you today to share my experience implementing FITARA as an Assistant Secretary for Information Technology and CIO at the Department of Veterans Affairs where I served from 2015 to 2017. I am pleased to join you and provide my recommendations to support the continued effectiveness of FITARA.

Prior to joining the VA, I spent over 30 years as a global leader in operations and technology in private industry. During that time I led organizations as large and complex as the VA. I had complete fiduciary responsibility and accountability for implementing world-class processes and technology. However, during the preparation for my role in the VA, I frequently heard about how difficult it was to execute IT projects in the Federal Government. The causes were numerous: one or two-year appropriations, complicated program budgeting, hiring delays, data center proliferation, cultural nuances, even technology procurement decisions being made outside the IT organization.

While I did witness each of the obstacles mentioned, within a short period of time, we were able to make progress at the VA. How were we able to do it? We had one critical strategic tool I could rely on. It was FITARA. FITARA is the law, and regardless of whatever obstacles I might have encountered, I had a law that I could leverage. I want to thank the committee for giving us that law and, therefore, the authority to act accordingly.

Let me share a figure with you, 74 percent of all main frame IT modernization projects fail. That's a staggering figure, and it is industry-wide. The primary reason is enterprise complexity and age. Many organizations obtain or develop new technology to enable a new process or solve a problem well before they understand how the solution will be supported or how the process will work.

In most cases you're trying to make something new work on something old. Integrating new technologies on top of old infra-

structure is always a risky proposition. The old infrastructure generally has not been well maintained. Therefore, unforeseen risks often occur and lead to subsequent failures. Just like the stuff in your attic or basement no one wants to get rid of anyway and no one has updated anything, the same thing happens in IT.

In addition to the infrastructure age, the organization's culture, and how it drives the use of technology, and the CIO's influence within the agency has a major impact on projects' success.

At Emerald One we address the issue of complexity by not just focusing on people, process and technology, but also engaging the leadership, being culturally aware, building trust, attaining the full value of the solution, and doing it in the shortest possible time so you can take advantage of the new technology. We call this the Elements of Brilliance.

With this in mind, I respectfully submit to the subcommittee several recommendations that I believe could strengthen FITARA.

The first recommendation is make the FITARA scorecard an agency-wide metric, therefore, providing the agency CIOs with the support needed to become the enabler of a critical agency asset along with the rest of the leadership team.

The second is to add a metric that measures the agency's average technology life cycle. This could be utilized to understand the risk of modernizing in that environment.

The committee should also consider a method to assess cultural readiness. The culture must be prepared to adopt new technology, not just endure it. Organizational leaders must focus on user adoption by measuring and managing the culture's preparedness before tackling any new technology.

And, finally, you must ensure that the agency's fiscal reality supports the technology mandates we impose. Many of our agencies continue to receive technology budgets that allow them to do little more than maintain and sustain outdated systems.

MGT supported by the TMF were both positive steps forward. By creating more meaningful connections between the mandates, the committee can create the leverage many CIOs need to modernize.

As the Chairman shared in his July 20th opening statement, we can no longer allow outdated and legacy technology to stymie the delivery of vital public services.

Chairman Connolly, Ranking Member Hice, and Members of the Committee, thank you again for the time and opportunity to share my experience and perspectives on FITARA. I look forward to its continued success and implementation and am happy to take your questions at this time.

Mr. CONNOLLY. Ms. Council, thank you so much; really very helpful observations from your own experience, very practical, and we look forward to working with you as we proceed. Thanks so much.

Mr. Spires, welcome back.

Mr. Spires?

STATEMENT OF RICHARD SPIRES, PRINCIPAL, RICHARD A. SPIRES CONSULTING

Mr. SPIRES. Yes, Mr. Connolly. Good afternoon to you——

Mr. CONNOLLY. Welcome back.

Mr. SPIRES [continuing]. Ranking Member Hice and Members of the Subcommittee. I'm honored to testify today in regards of FITARA and the scorecard that Congress has been issuing over the past five years.

Having served as the CIO of the U.S. Department of Homeland Security, as well as IRS, and having served as the Vice Chair of the Federal CIO Council, I had ample opportunity to understand the management dynamics inherent in Federal IT.

I was pleased when FITARA was enacted, but while the legislation itself has been of aid, I believe it has been the oversight of Congress that has been the driving factor in getting Federal agencies to improve their IT management.

In particular, the spirit of bipartisan has made a significant positive difference, starting with the drafting of FITARA, and it continues today with leadership from the subcommittee. Yet even with the progress, much work remains to reach the state of IT management best practice.

The hearing held by this subcommittee just two weeks ago showcased the need to continue to focus on IT modernization. But even if we had unlimited funds to invest in IT, many agencies would still struggle as they do not have the management maturity and skills to effectively deliver large scale IT modernization.

In 2015, GAO placed the whole Federal Government on its high-risk list for improving the management of IT acquisitions and operations. In GAO's latest report, it recommended that 12 agencies identify and plan to modernize and replace legacy systems, yet only three of the 12 agencies had implemented GAO's recommendation and made progress in even planning to modernize their legacy systems.

Given the success of the scorecard, it should continue as a tool to measure agency progress. I recommend changes to the scorecard to sharpen the focus on IT management and modernization, all of which are provided in my written testimony.

Some highlights of my recommendations include: One, add an IT planning category. Meaningful IT modernization starts with good planning and support by agency leadership. Hence, this category should reflect the maturity and focus on IT modernization within the agency's planning function and enterprise architecture.

Two, combine the incremental delivery and transparency and risk management categories into a broader delivery of IT programs category.

Agency IT modernization occurs through the successful delivery of IT programs and, as such, there should be a category that measures the ability of agencies in being able to manage such programs.

No. 3, evolve the managing government technology category to a broader IT budget category. This category should keep the element of an agency having an IT working capital fund. In addition, agencies should much better understand the cost element of the agency's IT budget. The Federal Government has adopted a Technology Business Management, TBM, taxonomy to support this effort.

Agencies should be measured on their adoption of TBM, along with the use of benchmarking of their IT services, so that they can compare themselves to other similar-sized agencies and private sector corporations.

Evolve the cybersecurity category. Agencies should be conducting meaningful enterprise cybersecurity risk management to ensure they are focusing on protecting their most sensitive data and critical systems. NIST has developed such a risk management framework called the NIST Cybersecurity Framework, the CSF, and its use is mandated by Federal agencies. Hence, the cybersecurity category should start with measuring whether an agency is properly executing the seven process steps of the next CSF.

Add a customer satisfaction category. IT organizations have customers. A core measure for all agency support organizations should be customer satisfaction. It would be best practice to administer a standard customer satisfaction survey to all agencies so this category can be added to the FITARA scorecard.

To determine the specific measures for a category and what additional data would be required for agencies to collect so the category could be graded, I recommend that Congress convene an advisory group that would develop recommendations to evolve the FITARA scorecard. This advisory group should be headed by GAO but include representatives from the Federal CIO Council, the Office of the Federal CIO, and from the private sector. Such an advisory group could make recommendations to Congress within three to six months.

Given the scorecard works, let's commit ourselves, as the Federal IT community, to evolve the scorecard to support and drive agencies to more rapidly adopt IT management best practices and move aggressively to modernize agency processes and systems.

Thank you for the opportunity to testify today.

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

And thank you, all three of you for your very thoughtful testimony. And I assure you, we'll be glad to work with you and take cognizance of some of the changes you propose in the metrics and in the scorecard itself.

The chair now calls on Mr. Palmer for his five minutes of questioning.

Mr. Palmer?

I'm informed Mr. Palmer is having a bandwidth issue. In Alabama maybe, huh?

Well, let me ask all three of you a series of questions. One is, how important is it that the CIO have the ear of the agency head? That's one of the categories we've actually added to the scorecard in terms of the reporting sequence, because from our point of view, it's about empowerment. If you're going to make decisions and make them stick, you know, the rank and file need to see that that CIO is empowered by the agency head, the boss.

In your experiences, how important is that, from your point of view? Maybe we start with you, Mr. Spires.

Mr. SPIRES. Yes, thank you, Chairman. Yes, I had the situation of reporting to the, if you will, agency head, a large bureau in the IRS when I was CIO, and not the case at DHS, actually. I reported to the Under Secretary of Management. So, I've seen both situations in government, and I think it makes a significant difference. And not to take away from the Under Secretary for Management in DHS, but that individual who I served under had no IT background and there was a lot of lost translation. And, frankly, I don't

feel like—not that I wasn't able to develop a relationship with the Secretary and Deputy Secretary of DHS, but it was not nearly as strong a relationship as I was able to develop with the IRS Commissioner. And I would say that, in my view, I was able to be more effective, significantly more effective, because I had a good relationship with the head of agency.

Mr. CONNOLLY. Ms. Council?

Ms. COUNCIL. Yes, I also agree with Mr. Spires. I actually, during my time in VA, even though it wasn't the norm, had a direct reporting relationship with the Secretary, who was Robert McDonald. Part of the reason for that was we had a short period of time to get a lot of things done. He understood I understood large enterprises. I had come from Johnson & Johnson. He had been at Proctor & Gamble. And it allowed us to sync very quickly.

It also is a way for the CIO to have the kind of support enterprise-wide that they need when an agency head is aligned with them. It doesn't mean that you don't include others in the conversation. It just means that everyone knows this mandate is a mandate. So, I totally agree with that alignment.

Mr. CONNOLLY. Thank you.

And Mr. Powner.

Mr. POWNER. Yes. So, I will third the importance of reporting to the agency head. I think it is very important the discussions we're having about mission modernization and tackling legacy where we have—where CIOs have relationships with the business leads and also a strong relationship with the CFO, so that there is the budgetary support to tackle these big, complex legacy modernizations.

So, having the support at the top so that they can be a business partner with the business unit and also having that strong relationship with the CFO is critical to tackling these big challenges the Federal Government faces.

Mr. CONNOLLY. Mr. Powner, while I've got you, maybe you heard the previous panel, our conversation about data centers and the attempt by OMB to maybe dilute the definition of data centers, which could have the unintended effect of losing savings and even compromising security.

Would you comment on that? Because you remember how important, the premium we put on data center consolidation when we actually began this process with the scorecard.

Mr. POWNER. Yes. No doubt, Mr. Chairman. So, a couple comments here. I knew when that memo came out that there was going to be a rub between OMB policy there and where you were going with data center consolidation. Do I think that we have had great success with data center consolidation? Yes, $4.7 billion in savings. Do I think there's opportunity to still do more? Sure, and populate with the capital funds.

I think what really needs to occur is I think there needs to be a really—there needs to be some type of agreement between OMB and what they're doing and what Congress wants to do, so you guys get more on the same page. Right now, right, we're at different ends of the spectrum here. I do think there's probably some coming together where you could tackle some data center. There's a lot that's already done, but there's still some opportunities.

That's why I think that the infrastructure category on the scorecard where you could still include data centers, but you also look at modern networks like with the EIS vehicle, is a good way to think more broadly about the infrastructure rate and how we tackle that.

Mr. CONNOLLY. You will remember, perhaps, that the very first hearing we had on this subject was when John Mica was chairman of this subcommittee, different kind of configuration. We had a field hearing at George Mason University in my district, and that forced people to look at how were they complying with this brand-new bill, FITARA, on data center consolidation. And what happened was we got much better at identifying thousands of data centers we didn't know we had, but we made zero progress on consolidation. Out of that hearing actually grew the idea of a scorecard, so we actually could create metrics and force action.

So, I hope we don't go back to that. It's distressing to learn that this action alone would take 2,000 existing data centers and basically take them offline. That's not the language of the statute and it's not the intent of the statute. So, it's worth watching.

And my time is up.

Mr. Hice, I recognize you for five minutes.

Mr. HICE. Thank you, Mr. Chairman.

Real quickly to each of you, and I don't want a long answer, just kind of get at your basic feel here, but I'd like to hear from each you as to how you think FITARA, the scorecard, has it been successful in driving change within agencies? From your perspective, is this thing working, and real quickly, why or why not?

Mr. SPIRES. I'll start, sir. Yes, it is definitely working. And as I mentioned in my testimony, the point is we've always had good people, good CIOs, you know, people that want to do the right things, but the environment in many agencies, the culture, as LaVerne was talking about, makes that difficult at times.

So, you shining a light on aspects of IT and IT management as congressional oversight, I think, is really critical, and it does force agencies——

Mr. HICE. Real quickly. I've got some other questions. I want to hear from the others. Yes or no?

Ms. COUNCIL. Yes. This is Ms. Council. I think it is working. I think it is working very well. I also believe that people manage what's measured. And because it's managed and because it's measured and because it's clearly transparent, it gets people focused on the right things.

Mr. HICE. OK.

Mr. POWNER. I agree with Ms. Council on, you know, what gets measured gets done. And I think what's really important to look at is your persistence and consistency. In most of these areas, it took at least four scorecards and two years to see significant change. We've got to stick with it in order to drive change, with some of the cultural issues that Ms. Council mentioned earlier; it just takes time.

Mr. HICE. OK. I don't know which one of you is most equipped to hit on this, but several of you or a couple of you brought this up with the CIOs. What's the biggest challenge that a CIO is facing

in the attempts to try to deliver large-scale IT modernization? What's the wall they're running into?

Ms. COUNCIL. I can take that one. Large implementations are just that, they're high risk and they're costly and they include people. And when you put all those together, you end up in the situation where you can't control all the aspects, and it requires a really focused effort of all hands on deck.

One of the biggest issues you run into, especially with one-, two-year money, even with the working capital fund, is that you may have multiple sets of these systems in the same environment. I can only speak to VA, but you're talking about one of the most complex environments in the world, not just in the U.S. Government.

So, when you go after trying to effectively change one of these, you've got to realize you're impacting an entire enterprise. None of these things are in isolation. None of these things easily are changed without engaging the entire whole. So, they are tough, but can they get done? Yes, they can get done. They require a lot of focus. They require everyone's intent.

And I think that's one of the reasons we think that the alignment needs to be the top of the house, so that everyone understands they have to have a stake in making it successful.

Mr. HICE. OK. Mr. Spires, are you there?

Mr. SPIRES. Yes, I am.

Mr. HICE. OK. You mentioned in your testimony—I'm sorry, my time is running out here, but you mentioned recommendations, if you will, regarding next steps for the scorecard, and specifically you brought up trying to phase in the metrics and obtain a buy-in from the stakeholders. Can you kind of walk me through what you have in mind when you make those comments.

Mr. SPIRES. Sure, Mr. Hice. I believe that we need to try to get better alignment. And Mr. Powner mentioned this earlier in an answer to a question about trying to get Congress working effectively with OMB, effectively with GAO. Let's come up with a set of metrics we all agree with.

They won't ever be perfect, but I think we can come up with a really good set of metrics. We've got to figure out how we measure them, that's important, and get the data. But if we do that and we can get better alignment—and this is a bipartisan issue, so I think we can work to do that. And I think we can make significantly more progress in driving IT modernization, because too often we're not going after it.

We're doing things that help, don't get me wrong, but some of the really big modernization efforts that do require that whole-of-agency effort agencies are just scared to go after, and we need to change that dynamic, because it's really important to our country that gets done.

Mr. HICE. Well, thank you. And I hope you're right. I agree, we need to—the metrics have been great, the question of the scorecard have been moving it forward to get more to the bottom line of what we need to get to. I think we can get there as well. I thank you for your answers and appreciate it.

Mr. Chairman, I yield back.

Mr. CONNOLLY. I thank the ranking member. And our hope I think eventually is to move to sort of a scorecard that is a digital

hygiene kind of scorecard, but it's important to note what Mr. Powner noted.

The only reason, in theory, we've made the progress we've made is because we have stubbornly insisted on the metrics contained in the scorecard for five years. And it took five years to get everyone finally better than a D and no Fs, five years. So, we want to be cautious about sliding back or assuming progress where it, frankly, has not yet been completely achieved.

So, I want to thank all of our panel for being here. There are so many other areas we could expand upon and——

Mr. PALMER. Mr. Chairman?

Mr. CONNOLLY. Oh, Mr. Palmer, are you still with us?

Mr. PALMER. Yes. I swiped myself off a little while ago.

Mr. CONNOLLY. Sorry. Welcome back. And you are recognized for five minutes, Mr. Palmer.

Mr. PALMER. Thank you, Mr. Chairman.

I want to go back to something Mr. Spires said about some additions to the scorecard, and this has to do with security. The Federal Acquisition Regulations are really written in such a way that cheapest is best, and it goes back to something that we talked about in that first panel about the fact that we're dealing with antiquated legacy systems, and about 51 percent of what we're buying is sourced from China.

So, I'm wondering if it makes sense to add to the scorecard and to encourage agencies to avoid buying—as much as possible, avoid buying from China. Mr. Spires, since you raised the issue of adding to the scorecard.

Mr. SPIRES. Yes. In the cybersecurity area, certainly I'm a huge believer in looking at enterprise risk. And there's no doubt today that cybersecurity supply chain risk is a very significant risk that we need to address.

So, I'm not in a position to say exclude—you know, shouldn't buy anything from China that's related to IT, but I think it is something that agencies need to take seriously as they look at their enterprise risk strategy. And I know that's certainly something DHS is looking at for all of government right now.

Mr. PALMER. Yes. I'm not saying that they can source everything outside of China, but we ought to encourage them to do as much as they can, because I think there's a gap, particularly when it comes to security, especially around this multitiered supply chain. And it's really mentioned nowhere or addressed nowhere in these acts.

So, let me ask it this way: Does it make sense to amend FITARA to assess the global supply chain security risk tied to the Federal IT acquisitions? Maybe that's where we start, and then we put that in—add that into the scorecard. Does that make sense?

Mr. SPIRES. Again, I go back to it is a key risk for enterprise cybersecurity for an agency, and it should be addressed as such. Whether or not that needs to be in legislation or just part of the scorecard, I think that's—I think that's why you should have an advisory group with some experts that are really—you know, that study this particular field, what would be best for the Federal agencies and how to handle this particular enterprise risk.

Mr. PALMER. OK. And I'm not totally familiar with all of the agencies, but I know there are a number of areas that are considered high risk. I don't know in the GAO's assessment if that includes high risk for security breaches in the context of where they sourced their materials.

Mr. Powner, do any of you—do you know?

Mr. POWNER. This question about high risk has come up a couple times, Representative Palmer. I think one of the key things we probably need to do here, whether it's supply chain or just high risk in regards to other aspects of high risk, you know, where there's risky acquisitions that are out there, it sounds like there's probably some clarification that OMB might need to look at in terms of their policies that they currently have in place so that we're all kind of singing off the same sheet here, because there seems to be a lot of confusion around this risk. And I would recommend that OMB take a good hard look at this high risk and look at what their policies say in those areas and perhaps clarify that.

Mr. PALMER. That's a great point. We will followup on that. And I think—I've been on Oversight since day one, I took a leave for most of this Congress, but I've done a lot of work with the GAO, and the thing that I want to commend the chairman and the ranking member on is we continue to work together in a bipartisan way to improve the quality.

In the previous panel, Chairman Connolly mentioned the fact that some of these agencies are still operating on COBOL. When I was in college, I was a COBOL consultant. And my concern is that there are not many people left who would know how to correct something if something went wrong with that.

So, there's a lot of vulnerabilities that exist. And I think what we're trying to do here, in a bipartisan way, is not only enhance our security, but also improve the quality of the work product by—what I think we need to be doing is replacing antiquated systems, and not only doing it at the Federal level but at the state level too, so that we've got that interoperability that we desperately need.

With that, Mr. Chairman, I thank you for recognizing me being back and being back on the committee, and I yield back.

Mr. CONNOLLY. Thank you, Mr. Palmer. Thank you so much. Very thoughtful.

Let me ask one last question, if I may, of all of the panelists, because given your experience. One of the things that concerns many of us is, especially those of us who are also in the private sector in IT, is that there's this gap, knowledge gap, experience gap, between the Federal Government and, let's say, the private sector, especially vendors who provide services to the Federal Government in this sector, and that that gap is almost growing. And to try to reverse that, we've got to be able to attract technology specialists and experts who can help the government manage its IT, procure its IT, and even as simple a task but not so simple, even writing the terms of reference for a complex IT contract.

I'd love to hear, as the final part of this hearing, your observations briefly about that problem, if you agree it's a problem, and what you think we ought to do about it.

Ms. Council, why don't you start.

Ms. COUNCIL. Thank you for the question. This is actually a question that impacts the governmental aspects as well as private industry. We don't have enough technologists anywhere. We don't have enough data scientists anywhere. We don't have enough architects anywhere. The need for technology, the need for people that really understand information technology and how to make it scale has constantly been there, but I can tell you now it's even tenfold.

As you see the now normal that we go through since COVID, technology is everywhere and it's everything. It allows us to be where we need to be, and when we can't be there physically, it allows our ideas to be there.

So, getting people to come work in the Federal Government, one, is really hard. I talked about that often when I was in the role. I wouldn't know how to get a job in the Federal Government. It's not a straight line. It's not sending a resume and you start talking to someone, as you would in a commercial entity.

It also requires that you know—you have to understand how to navigate. And I will tell you some of the best and brightest in our universities today, they are interested in working on technology, want to work on the newest things possible. They want to work on the hardest things possible.

So, I think the more we can give them that kind of environment, the faster we can get up on technology, the faster we can get new technology through FedRAMP, Chairman Connolly, the more excited young people will be, as well as some old people—don't count us all out. We know how to program, some of us do—will be more than willing to come in and help the Federal Government, no doubt about it.

Mr. CONNOLLY. Thank you.

Mr. SPIRES.

Mr. SPIRES. Yes, thank you. And great answer by Ms. Council. I'll build on that a little bit by saying that I really feel like—I mean, I came in mid-career into government at the IRS first, and I'll tell you the sense of mission is really palpable. And I don't think—I think we could do a much better job of enticing younger people if we would market ourselves better as Federal agencies.

I recognize that sometimes you don't have the latest technology that you can offer all of them, but I'll tell you, the opportunities that younger people can have that are talented, that really want to build a career, I think we're missing a big opportunity to be able to entice people. And I think if we marketed this more effectively, we could attract people.

Now, you're going to lose a lot of them, there's no doubt. I mean, maybe you have a program where you try to keep them for four or five years and help you. And some will stay. A lot will go back into the private sector, and that's OK. But we need to do something different. And I don't think we're going to be able to buy our way out of this with increased salaries, but I do think we have a wild card here that we need to play, and that's that sense of mission and the opportunities we can offer younger people.

Mr. CONNOLLY. Thank you.

Mr. Powner, final word.

Mr. POWNER. So, I agree on the sense of mission. Many times, IT departments in the Federal Government have this compliance focus, and that compliance focus isn't going to attract anyone. If you look at where Ms. Council was at, you know, who doesn't want to help the vets in our country or who does not want to help secure the homeland, where Mr. Spires worked.

Those are the types of missions we really need to get out front and to talk about the challenges that we face as a government and attract those young hard-chargers that are out there. It's not going to be easy because of the salary differences, but I do think—and we've seen it when you do have this mission focus. Like, why do some folks who are seasoned come back into government? Ms. Council did. Mr. Spires did. They come back because, you know, they're sold on the mission, and they want to actually help deliver on these missions.

It's no different with the younger folks we need to attract. We really need to sell the mission hard, because a lot of things in government are really important, and I think there would be a fair amount of people who would get behind that.

Mr. CONNOLLY. So, a little inspiration wouldn't kill us?

Mr. POWNER. Absolutely, absolutely.

Mr. CONNOLLY. Thank you.

With that, without objection, all members will have five legislative days within which to submit additional written questions for the witnesses to the chair which will be forwarded to the witnesses for their response. I ask all of our witnesses to respond as promptly as you are able. And I want to thank all three of you for really thoughtful contribution to this conversation and to the scorecard on FITARA.

And, with that, this hearing is adjourned.

[Whereupon, at 4:33 p.m., the subcommittee was adjourned.]