FITARA 15.0

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

DECEMBER 15, 2022

Serial No. 117–113

Printed for the use of the Committee on Oversight and Reform

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

U.S. GOVERNMENT PUBLISHING OFFICE
50–157 PDF WASHINGTON : 2023

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

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

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

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

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

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

RUSS ANELLO, *Staff Director*
WENDY GINSBERG, *Government Operations SubcommitteeStaff Director*
AIDAN MILLER, *Clerk*
CONTACT NUMBER: 202-225-5051

MARK MARIN, *Minority Staff Director*

C O N T E N T S

INDEX OF DOCUMENTS

FITARA 15.0

Thursday, December 15, 2022

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

The subcommittee met, pursuant to notice, at 11:01 a.m., in room 2154, Rayburn House Office Building, Hon. Gerald E. Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Brown, Hice, and Clyde.

Mr. CONNOLLY. The committee will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

I want to welcome everyone to the hearing which seeks to continue our oversight efforts of agency implementation and compliance with FITARA and other information technology laws.

Let me just say, I think this is our 16th—15th oversight hearing on a—on one law. I don't believe there is any precedent in Congress for that. I think we're unique, and it shows bipartisan commitment to making sure that FITARA is implemented and that IT modernization is the priority we recognized when we passed that bill into law. I credit GAO particularly for highlighting this issue as one of its high-risk categories, which Congress actually listened to and responded to and wrote a law to try to address it. Implementation, however, is key. Passing a law is only part of the process. Making sure that law is implemented is also really important.

We made changes to the scorecard. We created a scorecard to try to monitor and get metrics for that implementation. We have modified that scorecard, over the years, on a bipartisan basis. We've added more emphasis on cyber. We've also added more emphasis on personnel management issues like reporting in the org chart, who do you report to if you're the CIO. You know, we want to make sure that that person is imbued with the authority required.

Because of the interest of time, I'm not going to give any more of an opening statement than that. I will enter my opening statement into the record.

Mr. CONNOLLY. We are going to have votes starting at 11:30. Unfortunately, there are going to be four votes. If there was one, that would be easy. Four, that's not easy.

Eleanor Holmes Norton, when votes are called, would you be available to take the gavel?

Ms. NORTON. I certainly will.

Mr. CONNOLLY. You're wonderful, as always. Thank you so much.

I now call on the distinguished ranking member, my friend, Jody Hice, from Georgia. This is his last hearing as a Member of Congress. He's been a partner, and he's been sometimes a foil, but we've always—we've always been civil, and we have really tried to make as much music as we could together, and certainly in the realm of IT that we're talking about today, that has been the case.

So I thank Jody for his service to the American people, the people of Georgia, and call on him now for any opening statement he wishes to make.

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

If I could take a moment of personal privilege to respond to that. Likewise, it's been an incredible honor to serve in Congress for eight years and represent the great state of Georgia and the 10th District. To work with you, it's been a great honor, and I really appreciate working underneath the umbrella, specifically of Gov Ops here, and your desire really to make government work better for the American people, and all the efforts to find common ground. It has been an honor, and I wish you the absolute best, and your family, and a wonderful Merry Christmas as well. So I thank you for the opportunity.

Mr. CONNOLLY. Thank you, Mr. Hice, and right back at you.

Mr. HICE. OK. Thank you.

Mr. CONNOLLY. Thank you so much.

Mr. HICE. Yes, I'll just say, here we are again, 15th iteration of FITARA. We've got to have teeth to this thing. We've got to have some answers. Again, the administration, why they refuse to submit information as required by law is getting extremely frustrating, and I know you share that as well.

But I'll, likewise, forego my opening statement. I appreciate the witnesses being here.

Mr. CONNOLLY. Thank you, Mr. Hice.

Our first witness for today is the chief—oh, well—all right. I'll introduce and then we'll swear you in.

Our first witness is chief information officer for the Agency for International Development, Jason Gray. Welcome.

Our second witness is the Federal chief information security officer in the Office of Management and Budget, Chris DeRusha. Welcome.

Our final witness—actually, not our final witness. We have Carol Harris, director of information technology and cybersecurity at the Government Accountability Office. And she is joined by Jennifer Franks, also director of information technology and cybersecurity, to provide her thoughts on zero trust implementation. Our kind of implementation, zero trust.

Mr. HICE. And Ms. Franks is from Georgia.

Mr. CONNOLLY. Oh, Lord.

Mr. HICE. As she shares the Georgia nation, Go Dawgs.

Mr. CONNOLLY. All right. Well, that commends you too.

If our witnesses would rise and raise their right hand to be sworn in.

As you know, it's the custom of our committee and subcommittees to swear in our witnesses.

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

Thank you. You may be seated.

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

Without objection, your full written statements will be entered into the record. We ask you now for your five-minute summary, keeping in mind that when they call votes—yes. We can accept all the written statements. Oh, if you want—well, they may want to just say something briefly, and then we'll go to questions.

So if you can do what Mr. Hice and I just did, we'd appreciate that. Because we're just worried about time and we will want to get to substance just as quickly as we can.

Mr. Gray, anything you want to share with us briefly for the record?

STATEMENT OF JASON GRAY, CHIEF INFORMATION OFFICER, UNITED STATES AGENCY FOR INTERNATIONAL

Mr. GRAY. Thank you for the invitation to testify to you today. I will keep my comments brief. I do have prepared oral remarks, but because of the circumstances, I will keep them brief.

Mr. CONNOLLY. That will be entered into the record without objection.

Mr. GRAY. Thank you, Congressman. That is it.

Mr. CONNOLLY. Everything's fine at AID.

Mr. GRAY. Well, sorry, I have a five-minute written response——

Mr. CONNOLLY. All right. We'll come back to you.

Mr. DeRusha.

STATEMENT OF CHRISTOPHER J. DERUSHA, FEDERAL CHIEF INFORMATION SECURITY OFFICER, OFFICE OF MANAGEMENT AND BUDGET

Mr. DERUSHA. Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you for holding this important hearing on FITARA.

The FITARA scorecard plays a very important role in providing insight into the progress agencies are making to enhance their cybersecurity. I will keep my remarks briefer than I would have, but there are a few things——

Mr. CONNOLLY. Yes, Mr. DeRusha, you will.

Mr. DERUSHA. Just really quick, though, sir. The reality facing day one of this administration was we were weeks into one of the most significant events that our Nation's faced in SolarWinds. We realized the status quo approach to cybersecurity had failed us, and so we issued Executive Order 14028 to take some bold transformational actions there. Just a quick outline of that plan, and then I'll conclude my remarks.

You know, our transformation plan includes making our systems more defensible by employing zero trust principles; meaning, we've got to move so that trust is never implicitly granted. It must be continuously evaluated.

Across the Federal Government, we are replacing ineffective deterrents like passwords with multifactor authentication and

encryption. We're also leveraging the same methods used by our adversaries to continuously identify risks to Federal systems, to—and leverage threat intelligence so that we can prioritize remediation of those risks. Finally, we're working to infuse security design practices across new technology throughout the supply chain.

Just summarizing, much like that paradigm shift that we're working on in securing our networks, we've also begun to evolve how we measure success. So for Fiscal Year 2022, OMB and CISA have established a new baseline on FISMA metrics, many of which were selected around components of the EO. These data have been used to measure trends and work with agencies to identify areas where additional attention and resources are needed.

So, I look forward today to discussing that and what we've released on *performance.gov*. I'll also look forward to the opportunity to testify today and take your questions.

Mr. CONNOLLY. Thank you.

Ms. Harris.

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

Ms. HARRIS. I will keep my remarks brief.

Mr. Chairman, Ranking Member Hice, and members of the subcommittee, so we are here with the 15th iteration of the scorecard. It has just been a tremendous pleasure to work with you and your excellent staff as you continue, you know, your tremendous oversight of Federal IT issues.

I do want to take this opportunity now to thank the dedicated staff at GAO who do the behind-the-scenes work in putting the scorecard together for you. I don't know if you know this, but there are about 15 to 17 staff that support this effort. My then-assistant director, Kevin Walsh, led the first 11 iterations for you, and then Assistant Director Teresa Yost took over and has since led the last four.

I want to thank Teresa and Kevin in particular for their tremendous leadership, as well as our team at GAO for just their excellent work over these past seven years.

Now, just in terms of just—just very briefly, I did want to highlight a couple of things on the scorecard. So as you know, the overall grades for 17 agencies remain unchanged and have increased for seven. All 24 agencies have received a passing "C" or higher. And with Mr. Gray here, you'll see USAID remains the only one with an "A."

I do want to say a couple of positive things. Incremental development still appears to be very strong, according to the scorecard. Roughly 90 percent of agencies' software projects are being developed to using these best practice techniques which are called for by FITARA.

Another key positive mention is Portfolio Stat. The results of this effort have contributed to cost savings from moving the bar from $24.8 billion to $25.5 billion in cost savings and avoidances through Portfolio Stat. That is not insignificant. Again, I will reiterate, $25.5 billion is tremendous.

In contrast, when you take a look at the scorecard, I did want to mention EIS. There are 19 agencies that have an "F" here because they failed to meet GSA's goal to fully get off of the legacy contracts by September 30 of this year. There are variations across those agencies. There are a few that are closer to the 100 percent goal, but there are 17 that are less than 80 percent complete. And agencies need to act with tremendous urgency to move the bar here and get off of those legacy contracts as quickly as possible.

The legacy contracts are set to expire May 2023. GSA has already taken action to enable continuity of services through May 2024. We just don't want to have further delay because that is going to cause cost overruns. But the last transition was three years delayed and cost about $329 million in lost savings.

Finally, I just want to mention cybersecurity grades. They are, again, based solely on the Fiscal Year 2021 IG assessments. This means that there is an absence of cyber CAP Goals yet again for this hearing. I raised it last hearing. This absence is very troubling. OMB needs to take steps to remediate this gap immediately. We need to have clear and measurable IT CAP Goals because it's the law.

Finally, I just wanted to again mention my appreciation for working with you all these years. Thank you. I look forward to your questions, myself and Ms. Franks. Thank you.

Mr. CONNOLLY. Thank you so much.

Ms. Franks, you don't have testimony?

Ms. FRANKS. I do not.

Mr. CONNOLLY. OK.

And, Mr. Gray, given the fact that others had a minute or two, I do want to give you that opportunity. We didn't mean to cut you off.

Mr. GRAY. OK. I'd be happy to start a little bit, if that's OK. Thank you.

So, Chairman Connolly, Ranking Member Hice, members of the subcommittee, thank you for inviting me to testify today. USAID is grateful for your support, for our information technology innovation efforts, as well as our progress in complying with and integrating into the cultures the standards set out in FITARA.

When asked about the evolution of FITARA and the scorecard, from my years of experience across Federal agencies and long tenures as CIO, the yearend is always a good time to look at the past, the present, and where we want to go for our future.

In the past, the Federal IT environment was writhe with outdated IT infrastructure and little to no measurement or accountability of value for investment. The present environment shows the definitive impact that FITARA has had on improving critical technology modernization, security, and cost savings initiatives. Now, as the subcommittee looks toward the future of the scorecard, it will be important for agencies to look beyond FITARA as merely a grade and imbed FITARA holistically in the operational budget and performance structure of the entire agency.

I have been honored to serve as the CIO for USAID for four months; and prior to that, at the Department of Education for six years; and prior to that, several technology management positions in both the private and public sector. These experiences have

taught me that change is not only constant, can also be good. With change comes opportunity, experience, and expertise.

I would like to offer a few suggestions to the subcommittee on how to adapt or change the scorecard in the categories for the future, and I promise I will be brief.

For cyber, I would offer that there should be more than one metric, with all metrics aligning with the priorities Federal agencies are working on to better measure cybersecurity performance, and metrics should be regularly recalibrated to meet the evolving cyber landscape and reflect leading practices and standards of cybersecurity community.

For cost savings, when we look at cost savings and avoidance, over a three-year period, those cost ratios are based on both development, modernization and enhancement, DME, and operations and maintenance, which is O&M. Agencies may be penalized in that calculation by the money they are spending on modernization efforts. The measurement would be more accurate from a cost savings ratio if only the O&M were used to show the savings on "run the business."

And for DCOI, a better measure might be looking at the administrative and human capital burdens that are reduced, with fewer data centers mean fewer administrative overhead managing those data centers.

USAID looks forward to the continued benefit the scorecard and its measurements have provided to Federal CIOs and the clearly defined priorities that help agencies deliver mission outcomes, provide excellent service, and effectively steward taxpayer dollars on behalf of the American people.

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

Thank you for your time. I look forward to your questions.

Mr. CONNOLLY. Thank you.

The chair now calls on the distinguished gentlelady from Ohio, Shontel Brown, for her five minutes of questioning. Welcome.

Ms. BROWN. Thank you. Thank you, Mr. Chairman.

At our last FITARA hearing, we found bipartisan consensus on many things, including our disappointment with the administration's unwillingness to work with this subcommittee to provide meaningful and accurate data to score agencies' cybersecurity postures.

Ten of the 24 agencies received a failing grade last time. I am happy to report that for the past six months, we have worked with the Office of Management and Budget and Dr. DeRusha to develop cybersecurity metrics for the scorecard. Today, we offer agencies and the public a preview of a new meaningful cybersecurity metric.

So my question, Mr. DeRusha, can you explain the methodology behind these new cybersecurity metrics and why you think these are the correct metrics to incentivize agency best practices?

Mr. DERUSHA. Yes. Absolutely, Representative. I appreciate the question.

So the metrics that we put up on performance.gov yesterday are a good representative sample of where we've been focused in EO implementation. So, for example, if you look in the protect category, we focused on four things there.

One is ensuring we understand and are prioritizing risk as our adversaries look at our networks. We're talking about smart patching, which is using intelligence to prioritize our risk remediation.

Second, we're looking at multifactor authentication. That is one of the most effective ways to keep our adversaries out when they are knocking on the door.

And last, we focused on encryption. So if those defenses fail, you know, the harm is lessened or reduced to zero if you've got encryption in place.

So for us, we've been really focused on ensuring that we're putting the most attention in understanding where there may be gaps in implementation and opportunities for new policy interventions.

So, happy to continue to discuss our methodology beyond that, but those are the areas that I think deserve the most focus.

Ms. BROWN. Thank you very much.

Mr. Gray, how do you interpret the new metrics? Do you see them as an accurate reflection of your agency's posture and that they point you in the right direction as you seek to keep your agency on top of evolving threats?

The cybersecurity metric is unique on the scorecard by its nature, an effective approach to cybersecurity demands nimbleness and agility, an ability to predict and defend against evolving attacks and evermore determined adversaries. As a result, the scorecard cybersecurity metric has evolved over time using publicly available data to hold agencies accountable for making real progress in making their systems more secure. The need for transparency and access must be balanced against the legitimate need to protect sensitive data and information.

Mr. GRAY. Thank you for your question, Representative.

Mr. CONNOLLY. Mr. Gray, if you'll speak into the mic, closer. That's it.

Mr. GRAY. Sorry.

Mr. CONNOLLY. Thank you.

Mr. GRAY. Thank you for your—much better. Thank you for your question, Representative.

So I have as even during my opening remarks commented about the need for additional metrics for cybersecurity, because the FISMA scores that we get every year are great, but they're dated. So I am certainly an advocate for more metrics in terms of capturing the cybersecurity risk that agencies are able to manage.

So I think it's a good start. I know we've been briefed on it. Much like FITARA, I think—and look forward to it evolving over time. I know the CIO Council has been briefed on the metrics and the methodology.

I would say that for the metrics that are captured in what I have seen, yes, it is accurate as it relates to those metrics. I do think that there needs to be more, and even OMB stated this when it was briefed to the CIO Council, that it's going to mature. So I look forward to working closely with OMB and the CIO Council to look

for additional metrics that could be used to capture the holistic risk the agencies are managing every day.

Ms. BROWN. Thank you so much.

Mr. DeRusha, the Russia—the administration has prioritized zero trust as a bold and fundamental strategy to secure Federal information technology systems. Can you speak more to what a zero trust strategy involves and how this approach has been incorporated into the scorecard metrics?

Mr. DERUSHA. Yes. Absolutely, Representative. So our zero trust strategy's been based on extensive coordination with the private sector. This is essentially a security modernization strategy. What we learned in events like SolarWinds is that the old approach to being able to rely on our network boundaries as the perimeter of trust and then once you are vetted and in you can access resources freely, no longer works.

So what we're talking about here is focusing on a new approach to identity access management and control, and so that we are validating every user and device every time it tries to access a resource, to ensure that they are who they say they are, or the device is safe to operate in that environment. So it is really based around that and a number of other fundamental capabilities to ensure quicker detection of adversary activity.

Mr. CONNOLLY. Thank you. And thank you so much, Ms. Brown.

Ms. BROWN. Thank you.

Mr. CONNOLLY. By the way, Mr. Gray, if I were getting an "A", I would say the metrics are perfect, don't change a thing. But good for you in saying no, it's got to evolve.

The distinguished ranking member, Mr. Hice, is recognized for his round of questioning.

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

You know, the metrics have changed, but really nothing has changed. That's what's kind of disturbing to me. The data used to compute this scorecard was the same data that was used last year, and really nothing changed but the grade. And because—so a little more weighted approach to scoring.

For example, last year, the EPA got a "D." This time it got a "C", but nothing has changed; just the way we score. So we're not getting anywhere. We may pat ourselves on the shoulder and say, hey, we got better grades. But we don't have better grades, we just have a different way of grading, and nothing has changed from last year. That's disturbing to me.

Mr. DeRusha, let me ask you this. And we do have your written testimony and have looked through it. In there you mentioned 20 references to the President's executive order on cybersecurity but no references to the Cross-Agency Priority Goals. So this is, likewise, a bit confusing to me.

Is this administration, in your opinion, prioritizing an executive order over the Federal law that requires CAP Goals, No. 1? And No. 2, what is Congress supposed to do with this? Are we supposed to now prioritize an executive order over Federal law?

Mr. DERUSHA. So, Ranking Member, appreciate the question. The answer is they are both important. OMB's position is that we are complying with the law, and we made a decision to weave IT and cybersecurity throughout the President's Management Agenda

and several CAP Goals. We had a very aggressive executive order which we needed to measure our progress on. So we repurposed our FISMA metrics to really align with all of the goals and objectives that we've laid out there. For example, OMB has issued nine memoranda, nine cybersecurity policy memoranda, since the order was issued.

So we're very active and busy here. And there's just a whole body of work that we feel needs to be managed through that other process. But they are both extremely important.

Mr. HICE. Well, if they're both extremely important, why didn't you even mention CAP Goals? Why did you mention the executive order 20 times but not a single mention of the responsibility of Federal law?

I mean, this is backward to me. Just because there's an executive order does not give you nor anybody else the right to ignore Federal law, including the administration. It's time this stuff gets cleared up. The law is the law and it means something. It does not mean that we can ignore it.

I would think the chairman shares my frustration with this. The law is significant. It's the law, for crying out loud. Even in your own written statement, you ignored it and placed priority on emphasizing the executive order.

Let me—instead of the law—let me ask you this. You are now wearing two hats, the National Cyber Director and the chief information security officer. The NCD, relatively new, which, in fairness, I voted against it because it's confusing to me. It's like, what is it going to do? What is it supposed to do? And that was never clear to me. It's still not clear to me.

So if you could, in the two hats—the dual hats that you're wearing, explain what's the different between these two positions.

Mr. DERUSHA. So, Representative, my experience of being the first Deputy National Cyber Director, dual-hatted also as the Federal CISO, is that it's worked really well. Look, the Office of National Cyber Director is a brand-new organization. I think it's going to add a ton of value over a long term. Already we've seen it. You know, the office has grown to almost 75 people, and we're out there coordinating, communicating with the entire Nation and really getting everybody on the same consistent path toward, you know, modernization agenda.

So for me, being one foot in both organizations just ensures that we are congruent in all of our policy directions, so you don't have, you know, separate officials making different decisions. What that decision made was just kind of ensure that——

Mr. HICE. So which one is involved in policy?

Mr. DERUSHA. Well, I'm the same person, so they're both involved in policy in the end. But, you know, OMB generally still issues the policy memorandum per FISMA 2014 authorities, and we're just ensuring that Office of National Cyber Director staff are always aligned and supportive.

Mr. HICE. So is one more leaning toward policy and strategy or whatever, and the other more involved in enforcement, if you will, of the policies, or what——

Mr. DERUSHA. I would describe the No. 1 benefit of being in the NCD organization is that I'm aligned to and part of the entire orga-

nization's daily activities, so that I can stay apprised of where the entire strategic decisions are being made for the whole office and then bring that into everything that we're doing for Federal. So I—you know, that's kind of how I would just draw the distinction.

Mr. HICE. OK. My time has expired. It's still unclear to me.

Thank you. I yield.

Mr. CONNOLLY. Thank you, Mr. Hice.

The chair recognizes himself.

Mr. Gray, I know you've only been there four months, but you've got a perspective having come from a previous agency. I guess I'd invite you to talk a little bit about, how did AID do it?

I remember when AID got a low grade, and now you're kind of the archetype of how to do it and get an "A". So can you share with us a little bit your observation of what were the elements, management elements, resources deployed, personnel decisions, policy decisions, that went into AID taking a different direction and consciously so?

Mr. GRAY. Thank you for the question, Mr. Chairman. I would say that, while it has only been four months, I have certainly been on this FITARA journey for a number of years. The embrace by the agency of FITARA in totality—I have only been there four months, but there is not one week that goes by where FITARA is not referenced in one meeting or another. Focusing on cybersecurity or governance or modernization and the key tenants of FITARA has been fully embraced. Policy has driven it. Senior leadership's involvement has driven it. Resources being applied toward complying with and making sure that we are leading FITARA in implementing to really ensure that we're making better informed decisions.

I look at FITARA in a way like a navigational roadmap for a CIO, that you know where those critical landmarks are that keep you on track. And as it has evolved, those landmarks become clearer and we can measure month over month, day over day, year over year, to see, are we making it toward that goal.

So from what I have seen in the time is the full embrace of FITARA, it's not just a compliance activity. The outcome is better informed decisions, better management in terms of resources, and that's funding in individuals, and applying those resources to the appropriate projects and activities that are going to lead us to the future. That's what I would attribute.

The team has been phenomenal. I will share, and I was sharing earlier, that inheriting the team is just amazing. It's a phenomenal team that's fully embraced it, supported it, and is a hundred percent behind it, Congressman.

Mr. CONNOLLY. And obviously, for that to be successful the way you describe it, also requires the leadership to be fully onboard?

Mr. GRAY. Yes, Mr. Chairman. Absolutely.

Mr. CONNOLLY. Have you found that other agencies are approaching AID to say, how did you do it? I mean, is there some cross-fertilization going on? Is there curiosity, if not a desire to emulate, what AID has achieved in other agencies of the Federal Government?

Mr. GRAY. Well, I couldn't say that; I've been there such a short period of time. I will tell you that at the Federal CIO Council,

there's a lot of conversations specifically on lessons learned and best practices and how do we do this and how did you do that, which even myself coming in new, there were a lot of questions that I had of, how did you tackle this, and what was a really good way to manage this component or this part of FITARA.

Mr. CONNOLLY. Well, I guess I would urge you to document it. I mean, let's capture it and share it with other agencies, because you are a model. And while we want to talk about other metrics we may want to capture in a future scorecard, we don't want to lose the metrics we've got now and what they've accomplished. And you are an example of that.

Ms. Harris, did you want to comment on that from GAO's perspective, specifically about what AID has—the transformation they've gone through? And from your observation, how do they do it and why are they so successful, and can others emulate?

Ms. HARRIS. Well, I think Mr. Gray covered it very well. I think because they live and breathe FITARA and they have fully embraced it and they have executive leadership at the top that is fully promoting the important tenets of FITARA, that has made all the difference. And when you compare the agencies that are not doing as well as USAID, that is one of the key factors as to why, plain and simple.

Mr. CONNOLLY. Just calling it Connolly Issa just is so much easier than FITARA, but all right. That's a different subject.

Thank you. My time has expired.

Mr. Clyde, you are recognized for your line of questioning.

Mr. CLYDE. Thank you. Thank you.

I'm going to start off with a question regarding the new metric. And we'll go to GAO, Ms. Harris and Ms. Franks, in that order, if you don't mind.

What is your perspective on this new metric?

Ms. HARRIS. Well, I'm going to let Ms. Franks talk about the new metric.

Mr. CLYDE. All right.

Ms. HARRIS. But what I do want to go back to is the existing metric right now for cybersecurity is incomplete. It's not a perfect metric. It is not intended to measure cyber comprehensively. I think Mr. Gray is probably on to it, where you're going to have to have multiple metrics to give that holistic picture. But I think what's important is that these CAP Goals need to be addressed because it is the law. And having IT weaved into existing CAP Goals as an enabler is a great thing, but it is not what the law says. Real property and IT need to have standalone CAP Goals because these are longstanding IT management issues.

So I'm going to just mention that, but Ms. Franks will talk about the new metrics.

Mr. CLYDE. Ms. Franks?

Ms. FRANKS. Yes. I agree with Mr. Gray and Ms. Harris. So the metrics are not as comprehensive as one would think they need to be. So for an issue as complex and dynamic as cybersecurity, using a few selected measures cannot really just give us a holistic picture of what is going to be needed to really substantially paint this picture of what's going to be needed to fully and comprehensive give us what the Federal Government needs to fully comply with the

evolving cyber threats across the Federal Government, the sophisticated evolving events that plague us day in and day out.

So, what's going to be needed from these metrics is for OMB's guidance to give us that automated approach to really staying abreast of the cyber curve and really helping us to really fundamentally give us some up-to-date metrics. The smart patching, the multifactor authentication, the event logging, all of those are going to help us, but we really are going to need some metrics that are going to help all of the agencies with where they are.

All of the agencies' missions are different. They're fundamentally designed different. They're federated. They're just going to have to be designed differently for every single agency.

Mr. CLYDE. OK. Thank you very much.

Mr. Gray, USAID's cyber grade went from a "B" in the FITARA 14 scorecard to an "A" in today's scorecard. The improved grade reflects a change in the methodology as the scores in this scorecard are based on a weighted average. Consequently, the four attained by USAID, which was a "B" in the 114th scorecard is now presented as an "A" in this scorecard, as I see it. So I'm concerned that this appears to be simply a lowering of standards to show better results.

Do you see it this way too? Or if not, please explain.

Mr. GRAY. Thank you for the question, Representative. I think more work needs to be done, to be honest. I am so new to the agency, that I would be hesitant to respond specifically to the changes that have happened since last year and this year because it's only been four months. But I will say that the—there's a lot of activities that agencies are doing to manage risk that are not captured in a FISMA audit or even an additional cyber score, which really gets to my earlier point is that we capture a lot of data and look forward to working across government to figure out what is the right data to present the holistic risk associated with each agencies' portfolio.

So, I do think it's a great start. Much like I said earlier, the evolution of it is—and the maturation of it is really where we need to go so that we can truly represent the totality of what the metrics are showing us, because I have tons of metrics on a bunch of different activities that, in my view, is rather consistent across agencies. So——

Mr. CLYDE. OK. Well, thank you.

Mr. Chairman, I would like to take a moment of personal privilege in this last minute I have or so, and I want to thank my good friend and colleague, Congressman Jody Hice, for his leadership on this committee, as today is his last subcommittee hearing on Government Operations.

He's done an incredible job leading Republicans on this crucial subcommittee, and particularly the past two years during the Biden administration. Congressman Hice has stood for truth and conservative values. He's been a warrior in the fight for smaller and more accountable government. He's been a colleague of mine, and he has been my mentor.

Thank you.

Congressman Hice, you will be deeply missed, and you will leave very large shoes to fill. So thank you very much for your being here and your leadership, Congressman.

Mr. HICE. Well, thank you for those kind words, my dear friend. I deeply appreciate that. Thank you.

Mr. CONNOLLY. Thank you, Mr. Clyde. I certainly share your sentiments.

And before I call on Ms. Norton who's been so patient and kind, I want to thank my subcommittee staff for several years of extraordinary output. This subcommittee has had the most hearings of any subcommittee on the Oversight and Reform Committee. We've written the most letters. We've produced the most bills, by far, and that couldn't happen without capable, wonderful staff.

I want to thank Wendy Ginsberg, staff director; Annaliese Yukawa, my legislative assistant for this committee; Brian Maney, who is on loan to us as a fellow; and Asher Moss from Wesleyan University, who is interning with us. Of course, there've been people who've gone before who have done wonderful work.

I also want to thank Bill Womack and the Republican staff for usually their cooperation. Bill and I go way back to his former boss, and Tom Davis, who was the former chairman of this committee. I succeeded him in the 11th District of Virginia, and some day I hope to succeed him as chairman of the committee. But that's a different subject too.

I also want to thank Aidan Miller who is here with us today, who also worked in my office.

So, thank you all very much for wonderful efforts.

We're going to continue next year in the minority, hopefully temporarily, and hopefully we'll continue the tradition of this subcommittee in terms of bipartisan cooperation on this subject area. I've worked with Will Hurd; I've worked with Todd Platts; I've worked with Mark Meadows; I've worked with Jody Hice. We've got a long bipartisan tradition when it comes to trying to modernize IT and the Federal Government. And indeed, FITARA was co-written with Darrell Issa, also chairman of this committee, Republican chairman of this committee. So we want to keep that tradition.

We want to make sure that we are monitoring and setting the right metrics for progress to serve—better serve the American people and to make sure that we are cyber secure. And your input and your experience are really important. That's why we have these oversight hearings, not only to score people but to try to nudge them toward that progress that AID has been able to succeed at.

With that, the gentlelady, the Congresswoman from the District of Columbia, Eleanor Holmes Norton, is recognized for her round of questioning. Welcome, Delegate Norton.

Eleanor, you're muted.

Ms. NORTON. Thank you, Mr. Chairman. May I also applaud the extraordinary role you have played as chair on this committee.

And let me ask Mr. Gray a question. Mr. Gray, FITARA will require CIOs, and here I'm quoting, to have a significant role in the decisions, processes and management, governance and oversight process related to information technology, end quote.

Since the subcommittee added a CIO reporting authority metric on the scorecard, the percentage of CIOs with a direct or partial

reporting relationship rose from 50 percent to over 90 percent. CIOs have previously testified to how helpful FITARA was at giving them a spot in the C-suite conversations.

So, Mr. Gray, as a member of the Federal CIO Council, you have seen the transition firsthand. What are the benefits of having a direct reporting relationship to your agency head?

Mr. GRAY. Thank you for the question, Representative. I absolutely support the CIO reporting to the agency head for numerous reasons. For example—and I have been fortunate enough to hold this role in two agencies that reported directly to the agency head—the value is not just having a seat at the table, but it is ensuring that I am able, or this position is able to brief senior leadership on how are things going from a cybersecurity standpoint. How are things going from a government standpoint? How are operations going? How are we modernizing? What are we doing for user experience and customer satisfaction? How is the work force doing? And it gives that direct feed to agency leadership, so when they are needing to make decisions across the entire agency that go beyond technology, that they have that critical information to inform those decisions.

So it has been instrumental to ensure that I am able to give regular updates so that the agency head is informed and making the best decisions with the information that's available at the time.

Ms. NORTON. Well, thank you.

Now, Ms. Harris, Federal CIOs have a seat in the boardroom but may not have a voice in—at the decisionmaking table. So considering all this progress for Scorecard 15.0, the subcommittee is reviewing an evolution of this category to include additional metrics on the CIOs' influence on IT budget and acquiescing decisions.

So, Ms. Harris, GAO requested a report in the 2018 Federal chief information—on the Federal chief information officers. Could you briefly describe the results of that report?

Ms. HARRIS. Yes, ma'am. So the bottom line of the report is that none of the 24 agencies had policies that fully addressed the role of the CIO consistent with Federal laws and other guidance.

So there are roughly six areas of responsibility for CIOs. They include things like IT strategic planning, the IT work force, as well as IT budgeting, just to name a few. The agencies told us that CIOs are implementing the responsibilities in these areas even when they are not required by policy, but in our surveys to the CIOs, all of them acknowledged that they were not always very effective in implementing in those six areas. So there's a linkage of how critical it is to have it in policy at the agency, the impact, to empower these CIOs.

Right now, there are eight of the 24 agencies that have since addressed those policy gaps. So there are still 16 that continue to have gaps. We also made recommendations to OMB to provide additional guidance related to CIO authorities relative to the IT work force, as well as to providing a complete definition of the authority that CIOs should have relative to the IT spend.

So these recommendations remain open. That means that there is still work that needs to be done to fully empower CIOs. It is great that they have that seat at the table, they have that direct line reporting to the head of their—of the agencies, but there are

still additional responsibilities that they carry that need to be fully flushed out. So I am very pleased to see this category in the scorecard expanded to address some of those areas.

Ms. NORTON. Thank you. I see my time has expired.

Mr. CONNOLLY. Thank you, Ms. Norton. And thank you for making yourself available to chair the hearing, although it looks like we may not need to do that. But thank you so much for always being gracious with your time.

Let me followup on the last question just real briefly, Ms. Harris. At our last scorecard hearing, I believe we had some problems with OMB getting data to us, which then distorted scores for agencies. Has that issue been addressed?

Ms. HARRIS. Are you referring to the cybersecurity scores?

Mr. CONNOLLY. I believe it was, but the issue was OMB sitting on—either sitting on that or not providing it to the committee.

Ms. HARRIS. That's correct. The OMB did not provide that publicly as they are expected to do so. It's unclear to me whether they are sitting on that information or whether they just don't have that information. The main issue at hand is that there are, at this time, no specific IT CAP Goals. That is clearly and distinctly in the law, that they should have distinct IT CAP Goals as well as real property goals, and at this time, we don't see that coming out.

Mr. CONNOLLY. Mr. DeRusha, both Mr. Hice and now Ms. Harris have—have reminded us all, it's in the law. So can you address that issue on behalf of OMB?

Mr. DERUSHA. Chairman, I can. OMB——

Mr. CONNOLLY. Did you say I can?

Mr. DERUSHA. I can, sir.

Mr. CONNOLLY. All right.

Mr. DERUSHA. OMB's perspective is that we are complying with the law. If you look at the CAP Goals that we have woven IT throughout, they're all focused on digital delivery, right, and they've got security principles and the best of IT delivery, digital delivery principles embedded throughout. So I think we do feel we have that.

But the important thing to us is that, again, I said nine—nine policies we've issued. I mean, there's been a huge emphasis in body of work. Yesterday we released the performance metrics on performance.gov for cybersecurity. We are very open to continuing to evolve those. That is our plan. We've adjusted some of our metrics for 2023. We're open to continuing conversations with the committee on other focus areas.

So, you know, our view is that it's important that we've got the metrics out in public, and we're going to continue to evolve this as we go.

Mr. CONNOLLY. So at our next—I don't think GAO is satisfied with that answer.

Mr. HICE. No, neither am I.

Ms. HARRIS. Mr. Chairman, if I may?

Mr. CONNOLLY. Neither is Mr. Hice.

Ms. Harris.

Ms. HARRIS. The law clearly states that these IT CAP Goals need to be standalone in order to address these longstanding IT management challenges that we face. It's a great thing that OMB has in-

fused and weaved technology into these other CAP Goals to use IT as an enabler for, for example, customer experience. All for that. But it's not—and digital delivery. But it is not addressing these longstanding issues that we have had with IT relative to cybersecurity and IT management.

Mr. CONNOLLY. OK.

Mr. HICE. Mr. Chairman, if I could just add.

Mr. DeRusha, just remember you are sworn in under testimony. And to say that you are abiding by the law, I would be very, very careful, because you probably are alone in that opinion.

Mr. CONNOLLY. I would simply say, we—by the time we have our next FITARA hearing, hopefully, Mr. DeRusha, OMB, and hopefully Ms. Harris, GAO, can reconcile these approaches and make sure they're constant with the law. And the end goal here is to be able accurately to measure progress, and that's why it's in the law, and so we want to make sure that works. So we thank you for that.

Mr. Hice, anything more for the record?

Mr. HICE. I'm good. Thank you.

Mr. CONNOLLY. Really?

Mr. HICE. Yes, sir.

Mr. CONNOLLY. All right. Let the record show he's good.

At any rate, I wish everyone happy holidays. Thank you so much for coming to our 15th hearing on OMB, and I assure you—I mean, excuse me, on FITARA, and I assure you, it will not be our last. Happy holidays, everyone.

We are adjourned.

[Whereupon, at 11:51 a.m., the subcommittee was adjourned.]

○