FITARA 13.0

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JANUARY 20, 2022

Serial No. 117–61

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

46–682 PDF WASHINGTON : 2022

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
VACANCY

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

CONTACT NUMBER: 202-225-5051

MARK MARIN, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

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

C O N T E N T S

NO ADDITIONAL DOCUMENTS WERE ENTERED INTO THE RECORD FOR THIS HEARING.

FITARA 13.0

Thursday, January 20, 2022

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

The subcommittee met, pursuant to notice, at 9 a.m., via the Zoom video platform, Hon. Gerald Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Lynch, Khanna, Porter, Brown, Hice, Keller, Clyde, Biggs, and LaTurner.

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

For the past six years, this subcommittee has maintained steady and bipartisan oversight of agency implementation of FITARA, the Federal Information Technology Acquisition Reform Act.

In addition to other critical IT-related statutes and executive branch IT priorities that are incorporated into the biannual FITARA scorecard, we have provided vigorous oversight.

In practice, the scorecard is a tool for Congress, chief information officers, agency heads, and outside stakeholders to understand how Federal agencies across the enterprise of government are performing in various IT acquisition categories.

Since the scorecard was first released in 2015, it has driven positive change in information technology system acquisition and management across 24 Federal agencies, and it is estimated by GAO that it has saved taxpayers more than $20 billion in improving the security of Federal IT systems. There aren't a lot of other bills that have saved the Federal Government that much money.

This subcommittee, regardless of who is in the majority, has held more oversight hearings on FITARA in the last seven years than on any other Federal piece of legislation. As we will hear today from the Government Accountability Office, the scorecard has served as an effective oversight tool since its very inception.

From November 2015 through December 2021, agencies receiving C or higher grades increased from 29 to 100 percent, and for the most recent scorecard, 50 percent of the agencies received an A or B.

To continue driving progress, the scorecard needs to evolve to reflect the changing nature of IT services and to guarantee that we are accurately assessing modernization and IT management practices of Federal agencies.

The goal here is to incentivize progress, not to get a gold star on our foreheads. At today's hearing, the subcommittee will hear diverse perspectives on the scorecard including opportunities to upgrade its categories and metrics for more focused and objective measurement of agencies' performance.

Since the July 2021 FITARA 12.0 scorecard, seven agencies' overall grades increased, four decreased, and 13 remained unchanged. These grades resulted in all agencies receiving a passing C or higher grade for this round's scorecard.

In the data center consolidation category, every agency received an A grade based on the scorecard's current methodology. As such, the fourteenth scorecard will retire this methodology when it is released later this year.

Today, the subcommittee grades agencies using each agency's quarterly data center submission to the Office of Management and Budget and weights that data center grade according to the subcommittee's priorities.

I want to congratulate agencies for getting all A's in this category. But that is not to be construed as a mission accomplished moment, by any means.

Given the subcommittee's oversight history on Federal data center consolidation, we approach this accomplishment with a bit of a jaundiced eye.

We look forward to hearing from our witnesses today on ways the subcommittee can continue to hold agencies accountable for the efficient data center consolidation and transition to the cloud.

Data center consolidation category is one example of a larger trend that points to the need to upgrade the scorecard. While no agencies earned an F grade since 2018, on average less than 10 percent of agencies are achieving an A grade and 53 percent are showing no change to their overall grade over time. That's not progress.

Agencies appear to be less motivated to improve grades, perhaps, because of the methodology used to calculate some of the metrics. For example, two of the metrics are graded on a curve, which can be received as counterproductive to an agency's ability to demonstrate improvement during the scorecard cycle.

A variety of factors including methodology, data availability, agency motivation, and the cycle of the scorecard have resulted in stalling grades for many agencies.

The subcommittee is at an inflection point, and the time is right to modernize this oversight tool. The Federal Government spends more than $100 billion each year on IT investments.

GAO has found that, historically, the projects supported by these investments have often incurred multimillion-dollar cost overruns and years-long schedule delays. In addition, they may contribute little to mission-related outcomes and, in some cases, fail altogether.

Congress enacted FITARA on December 19 of 2014 to ensure focus, discipline, and consistently effective management and to codify existing administrative initiatives to improve Federal IT managed by Federal CIOs.

Key pillars of the FITARA scorecard including cybersecurity and IT modernization remain on GAO's high-risk list, highlighting the need for vigorous and continued oversight on these issues.

To conduct such oversight effectively, the FITARA scorecard must accurately reflect the progress agencies have actually made in their IT efforts, which will, in turn, motivate agencies to prioritize meaningful changes.

This subcommittee is prepared to lead the way on FITARA's evolution. Expected updates to agency IT data, reporting requirements, and upcoming revisions to the IT dashboard provide an opportunity for us to enhance and upgrade the scorecard itself.

Moreover, FITARA 13.0 marks only the third time in the scorecard's history when government had only two acting CIOs—the Department of Interior and the Department of Health and Human Services.

All the rest have been made permanent or confirmed. So, we have a cadre of permanent CIOs who we count on as trusted partners in driving transformational change to improvements at agency IT systems.

Congress must use metrics that empower and incentivize CIOs to improve Federal IT and we must collectively avoid bureaucratic gaming by cherry picking metrics that enable agencies to inaccurately inflate performance. Working in lock—because the goal is to capture real progress or not.

It is not to get a gold star on the forehead by kind of playing games with the metrics nor is it to get a scarlet letter on our back because we fail to meet some goals. We want to better capture how are we doing, how can we improve, what do you need.

Finally, the subcommittee will not waver in its continued oversight of agencies' IT acquisition and management. We must continue to reap dividends from modernizing legacy IT systems, migrating to the cloud, maintaining strong cyber postures.

Congress and the administration must work together to prioritize IT modernization and cybersecurity across the Federal Government to maintain our commitments to everyone we serve, especially now during a pandemic.

The chair now recognizes the ranking member for his opening statement.

Representative Hice?

Mr. HICE. Thank you, Mr. Chairman, and you have got me curious what your tie is this morning.

Mr. CONNOLLY. It is Franklin Delano Roosevelt. My sister got it at Hyde Park at his Presidential library.

Mr. HICE. Very nice. I would like to see it——

Mr. CONNOLLY. And he is—as you know, he is the Georgia connection at——

Mr. HICE. Absolutely. Absolutely.

Thank you, Chairman Connolly, and I appreciate this opportunity to yet again monitor the massive Federal Government IT spend, and I also want to extend our thanks to the witnesses who are—to both panels who are here with us today as we discuss the thirteenth—for the thirteenth time the most recent iteration of the FITARA scorecard.

I would like to touch on two areas that stand out on the current scorecard. First is the data center consolidation and then the Enterprise Information Solutions, or EIS.

First of all, does the data center consolidation matrix still serve a purpose today? I think that is a fair question, something that we really need to consider.

And, certainly, absolutely, don't get me wrong, Mr. Chairman. The early stages of FITARA, no question this metric was relevant, it was forward looking, and it dealt with efficiencies and savings within our agencies.

But with all the agencies now receiving an A on this current scorecard, I think it is a fair question as to whether, indeed, we have reached a point of diminishing returns and need to legitimately consider where do we go from here.

And, Mr. Chairman, you and I have talked about this many times. I appreciate your strong feelings about this issue and your view that the good grades, perhaps, reflect a good move in the right direction.

But I am eager to hear today from our witnesses as to whether there are valid reasons for us to, perhaps, shift our focus elsewhere and go to the next level.

With respect to the Enterprise Information Solution metric, again, I think we have to ask what's happening. Fifteen of the 24 agencies are failing, and I hope we can get answers as to why this is the case and how this subcommittee can get things back on track.

Beyond the current scorecard, I believe it is time to take a hard look at how FITARA can evolve from this point. During last week's FISMA hearing, I specifically asked the GAO witness whether the current FITARA metrics give an accurate picture of the agency's security posture, and the clear answer was no.

So, I think, again, that is an indication that we need to evolve and go to the next step, and I am curious as to the panelists today what their thoughts in that regard may be.

Of course, we are all aware of recent cyber-attacks such as SolarWinds and Log4j. We have got ample illustrations as to our vulnerability. Not that we need reminders. There is plenty of them out there.

But security is, absolutely, one of the top areas for oversight. We need to keep that as our priority and we here in the subcommittee need a clear picture as to how safe agency systems actually are. I think that is a concern for all of us and we, I believe, need to perhaps evolve more into that direction.

As we look forward, taking advantage of the effort to update the underlying FISMA law, we should reexamine the scorecard metrics and think about how cyber assessments can better serve our purposes, and there are, certainly, areas that are not reflected in the scorecard that I believe we at least should consider, such as the state of Federal IT modernization, such as work force issues.

Another point is customer satisfaction. All these things we have discussed in the past. But are these IT dollars actually delivering results for our constituents? Again, I am eager to hear from our witnesses today on all of these and other issues.

I think a related question is, is twice a year the right cadence for this review? Does a six-month interval actually give agencies enough time to change course if they need to? Are there other reasons to move this, perhaps, to an annual event?

So, I look forward to working together—Republicans, Democrats, Federal agencies, private sector, all stakeholders—to improve our oversight mechanisms to ensure Federal IT is efficient and safe.

Again, Mr. Chairman, I thank you for your commitment to this issue and I look forward to today's testimoneys. And with that, Mr. Chairman, I yield back.

Mr. CONNOLLY. Thank you, Mr. Hice, and I want to assure you that I agree with you. I think we have to update the scorecard to make sure that it is accurately capturing progress or lack thereof, and identifying issues as they evolve, too, including new issues. And I don't think anyone could look at current Federal performance and say, everyone deserves an A and everything is going wonderful. And so we need a scorecard that captures the good, the bad, and the ugly.

And I, certainly, look forward to working with you and making sure that as we modify, you know, the scorecard, it is done with an eye toward capturing what matters in an accurate way. So, thank you.

Let me introduce—we have two panels, and what I am going to do is kind of consolidate them. We will go—the reason being I am very worried about the weather, and I am very worried about votes, and we are going to lose members once votes are called. And I also don't want to have to recess the hearing if I can help it and put a burden, especially, on the second panel.

So, on our first panel we have Ann Dunkin, who is this chief information officer for the Department of Energy; Guy Cavallo, chief information officer for the Office of Personnel Management; and Carol Harris, who, of course, is with us again as the director of information technology and cybersecurity from the Government Accountability Office.

On our second panel we have three friends who are very familiar to this subcommittee and to Congress: Dave Powner, formerly of GAO, now executive director of the Center for Data-Driven Policy at MITRE; Suzette Kent, former CEO—I am sorry, former CIO for the Federal Government and now CEO of Kent Advisory Services; and Richard Spires, formerly a CIO for the Federal Government in several agencies and now principal of Richard Spires Consulting.

If all six of our witnesses would virtually rise and raise your right hand to be sworn in and unmute yourself.

Do you swear to tell the truth, the whole truth, and nothing but the truth, so help you God?

[Witnesses are sworn.]

Mr. CONNOLLY. Let the record show that all six of our witnesses answered in the affirmative, and I thank you so much. Without objection, your written statements will be made part of the record.

And with that, Ms. Dunkin, you are recognized for your testimony.

STATEMENT OF ANN DUNKIN, CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY

Ms. DUNKIN. Good morning. Chairman Connolly, Ranking Member Hice, and distinguished members of the committee, it is an honor to appear before you representing the Department of Energy.

On behalf of Secretary Granholm and Deputy Secretary Turk, I thank you for providing me this opportunity to testify about DOE's implementation of the Federal Information Technology Acquisition Reform Act.

I would like to thank the subcommittee for its leadership and bipartisan oversight of agency implementation of FITARA, which has enabled us to make real progress at DOE, progress that I am excited to buildupon as the department's CIO.

I am thrilled to return to government as DOE's CIO and to work again with my highly capable and mission-driven Federal colleagues. I report directly to the secretary and deputy secretary, and I have their full support to drive change and make enterprise decisions as I implement FITARA across DOE, accelerating our technology, innovation and cybersecurity efforts across our unique operating environment.

Although we have made significant progress, I acknowledge that we still face challenges. I am committed to driving progress on this important work and I look forward to working with you to do so.

DOE's governance framework, with the highest body chaired by Deputy Secretary Turk, is our vehicle for fully implementing FITARA, helping to ensure our IT and cybersecurity programs are strong enough to support and enable Secretary Granholm's three major priorities: combating the climate crisis, creating clean energy union jobs, and promoting energy justice.

As the DOE FITARA program continues to mature, including at our national laboratories, Power Marketing Administrations, plants, and sites, we will continue to focus on the following: enhancing our visibility to IT-related resources and investments, supporting CIO and IT management authorities at all levels, improving our cybersecurity posture, implementing new and updated policies for managing IT, and strengthening governance and oversight processes.

That is the big picture. Zooming in, I want to highlight the progress we are making in a few key areas.

DOE is working to close seven more data centers by 2025, adding to our total of 146 data centers closed so far. I am committed to enhancing the energy efficiency and sustainability of our remaining data centers. The MGT Act is critical to the innovation efforts I am leading at DOE and in my capacity as the CIO Council's Innovation Committee chair.

Across the Federal Government we use DOE's existing Working Capital Fund for some IT acquisitions and we are exploring the creation of another for IT modernization.

DOE continues to make progress toward improving our cybersecurity posture. Various security needs within DOE's mission space present unique cybersecurity challenges requiring our risk management program to be flexible and allow for risk-based decision-making to enable our mission.

The department is leveraging the Department of Homeland Security's continuous diagnostic and mitigation program to obtain additional security tools, including most recently Hardware and Software Asset Management.

These capabilities will provide added visibility to support risk-based decisionmaking. DOE has also made investments in vulnerability management, big data analytics, crowd sourced penetration testing, and enhanced training initiatives.

We are looking forward to the new Fiscal Year 1922 FISMA risk-based approach to cybersecurity, which will allow DOE to focus on our highest priority mission areas and risks.

Another major priority for DOE is our work force. We are implementing a multi-pronged approach to compete for talent and I am proud to report that we recently launched the Omni Internship Alliance, a paid internship program for students from overburdened and underserved communities that will help build the cyber and IT talent pipeline that we need.

Looking ahead, I am encouraged by recent history. The government's response to the COVID–19 pandemic showed that we can move at the speed of need when lives depend upon it and when we remove cultural and process constraints.

While pandemic-induced crisis is not a path forward, this experience has inspired us to double down on our efforts to improve DOE's IT and cybersecurity posture, to remove barriers to innovation at scale, and to lead change across the Federal Government.

I said before that FITARA helps CIOs make government better. I still believe that FITARA laid the groundwork for CIOs to change cultures and enable greater collaboration and agility, and I am committed to driving that forward.

Drawing on these lessons we have learned about accelerating real transformational change, I am confident that with my team's commitment, dedication, and passion, and with the leadership of Secretary Granholm and Deputy Secretary Turk, we will achieve significant results.

I pledge to you today that we will be relentless in our work to strengthen the department by continuing to effectively promote FITARA, and I look forward to working with each of you as we proceed.

Thank you for the opportunity to testify before you today and I will be pleased to address your questions.

Mr. CONNOLLY. Thank you, Ms. Dunkin, and kudos on still pursuing data center consolidation. I am glad to hear there are seven more you are focused on. Thank you.

Mr. Cavallo, you are recognized for your opening statement.

STATEMENT OF GUY CAVALLO, CHIEF INFORMATION OFFICER, OFFICE OF PERSONNEL MANAGEMENT

Mr. CAVALLO. All right. Thank you, Mr. Chairman.

Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you for the invitation today to discuss FITARA and how it has helped drive OPM's modernization efforts to enhance our service delivery to Federal employees, retirees, their families, along with other Federal agencies and our citizens.

It has been 18 months since my predecessor, Clare Martorana, provided this subcommittee with an update on OPM's FITARA status. In the time since that hearing, we have implemented many of the necessary enterprise building blocks to accelerate OPM's modernization and to further improve our FITARA scores. We are proud that those efforts are paying off as validated by our recent improvement to a B+ on the scorecard.

One of the first building blocks was to assemble a CIO executive leadership team designed to meet today's technologies and challenges.

In the past year, I have added a number of key executive positions, including a chief technology officer, an enterprise architect, a cloud and cybersecurity senior advisor, and a digital services team lead.

Additionally, I reclassified our chief information security officer to become a Senior Executive Service position. Not only with that, but I have also aggressively pursued hiring our staff, and I am pleased to announce that we have reduced our vacancy rate by about 20 percent from the beginning of Fiscal Year 1921.

With those additional executives and staff in place, my team are pursuing technology modernization initiatives across many areas. An important foundation for application modernization is developing a total life journey map of a Federal employee's career, from applying for their first Federal job to being hired, to moving to a different agency or, perhaps, a different role, to potentially having a break in service, and eventually, at some point, they will become a retired Federal employee.

That journey map will help guide us in all of our modernization efforts at OPM.

Another key transformation effort this last past year was establishing OPM's enterprise cloud. I am a very strong advocate of the advantages of leveraging the capabilities of the cloud to improve the delivery of citizen services, and I have successfully implemented the enterprise cloud at two previous Federal agencies, and I am proud to now also have done so at OPM with the launch of our cloud earlier this month.

Another key modernization initiative was to replace our on-premises retirement services contact center with a flexible, expandable, cloud-based center designed to handle the high volume of inbound telephone calls.

This new service was launched just in September and it has already improved the contact center's performance and provides us with the ability to expand call lines as needed.

Next, to increase our transparency and risk oversight of OPM's technology investments, we reinstated our Investment Review Board. That board is helping to establish an enterprise-wide approach to technology, help us eliminate fragmentation, and to align our IT investments to OPM's core mission requirements.

A final area that I want to highlight are the steps we have taken to support the OPM work force in this new hybrid world of work. Through standardizing on an enterprise collaboration solution, we can now easily communicate internally and externally across OPM.

This has further allowed us to reduce duplicative software costs by consolidating multiple collaboration tools into a single enterprise solution, thereby saving taxpayer dollars.

Well, the work that I have highlighted here this morning is just a small subset of what we have already completed. At OPM, we will continue to use the FITARA framework as we enhance our IT modernization by implementing an enterprise-wide approach to technology.

Notwithstanding these efforts, I acknowledge that we still face challenges modernizing OPM's legacy systems as we continue to work to improve that customer experience.

Again, Mr. Chairman, thank you for the opportunity to testify on FITARA and for the committee's continued leadership in measuring the effective use of technology in the Federal Government.

I look forward to answering any of your questions.

Mr. CONNOLLY. Thank you very much, Mr. Cavallo.

And Carol Harris from GAO, welcome.

STATEMENT OF CAROL C. HARRIS, DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, 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 thirteenth set of grades. Per your request, my remarks will focus on the evolution and effectiveness of the biannual scorecards.

Mr. Chairman, as you know, the first two scorecards focus exclusively on four major components of FITARA: incremental development, risk management, portfolio stat savings, and data center consolidation.

The third scorecard included the CIO reporting path. The software licensing and working capital fund areas were added in scorecards five and six, respectively. Cybersecurity was added in 2019 in scorecard eight, and finally, the Federal telecommunications transition was added last year with the eleventh iteration.

There is no question that the release of these scorecards and your related oversight hearings have made a huge difference in improving the landscape of Federal IT.

Since the release of the first scorecard in 2015, we have seen a steady improvement in grades from seven agencies receiving a C or higher to all 24 agencies in that camp.

Mr. CONNOLLY. I am sorry. I am sorry, Ms. Harris. Did I hear you correctly that these hearings and our legislation has made a huge difference?

Ms. HARRIS. That is correct, sir. Yes.

Mr. CONNOLLY. I just wanted to make sure. Sorry. I wasn't sure I heard.

Ms. HARRIS. As well as the Connolly Issa Act.

[Laughter.]

Ms. HARRIS. In fact, half of the agencies have an A or B in this latest set. The escalation in grades reflect the notable improvements agencies have made in most of the scorecard categories.

For example, when software licensing was first added, only two agencies had comprehensive inventories that were used for decisionmaking and given an A. Three years later, all 24 agencies received A's in this category.

As such, the category was retired from the scorecard. Similarly, we have the first ever straight a performance by the agencies in the data center category. Since 2010, the agencies have closed almost six,800 data centers and achieved $6.6 billion in savings.

The rate of consolidation has slowed and it will continue to taper down. Thirteen agencies had zero planned closures in Fiscal Year 1921 and an additional seven agencies are not planning for future closures.

Looking at Fiscal Year 1922 and beyond, seven agencies plan to close 79 more centers and save a total of $46 million. Consolidation has slowed because we have squeezed as much juice as we can from this initiative.

In contrast, the vast majority of agencies are not moving fast enough in their transition off of GSA's expiring telecommunications contracts. These contracts expire in May 2023.

Fifteen agencies have an F in this category, and it is worth noting GSA is one of those agencies. As the one responsible for the successor program known as EIS, they should be leading the pack as the role model.

The transition previously took three years longer than planned, and had the agencies transitioned on time they would have saved about $329 million.

Now, turning to the future of the scorecard, we believe it needs to evolve in order to maintain its effectiveness as an oversight tool. On average, roughly, half of the agencies have had no change to their overall grade, and while it looks like the agencies have fallen stagnant, I don't believe this is the case.

Agencies are increasingly less motivated to improve in areas where they are being graded on a curve and that is risk management and portfolio stat savings, and, as such, these methodologies should be changed.

Regarding cyber, this category should be expanded to better address the ongoing and emerging challenges facing our Nation, including mitigating global supply chain risks and improving the implementation of government wide cybersecurity initiatives.

We have recent work in each of these areas that would support a potential expansion in this category.

And finally, we should consider adding a category that directly tackles the legacy IT issue. Roughly, 60 percent of the more than $100 billion spent on IT annually is put toward maintaining antiquated systems.

Your persistent leadership on the working capital funds and the Technology Modernization Fund has helped agencies to be better positioned to tackle this problem.

The next logical steps should be tracking agency progress in decommissioning their most critical legacy systems.

We have appreciated the opportunity to be your partner all these years in developing the scorecard, and we look forward to supporting your efforts to ensure that it remains an effective tool in improving the management and security of our Nation's IT.

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

Mr. CONNOLLY. Sorry. Thank you, Ms. Harris. Thank you for GAO's long partnership in working with us on the implementation of this legislation.

We are now going to hear the testimony of Panel Two. We will be liberal in the amount of time people need because we are consolidating the two panels because of the weather and because of the vote schedule.

But I urge people not to abuse that because we want to try to give everyone an opportunity to participate in the hearing, because you and I both know once they call votes and it is, you know, a fly out day, we are going to lose people, and I want to maximize the opportunity for everybody to participate.

I will, of course, go last so that my colleagues will have an opportunity to ask their questions.

So, Mr. Powner—an old friend, a familiar face—you are recognized for your five-minute opening statement. Welcome back.

STATEMENT OF DAVID POWNER, EXECUTIVE DIRECTOR, CENTER FOR DATA-DRIVEN POLICY, MITRE, FORMER DIRECTOR, INFORMATION TECHNOLOGY AND CYBERSECURITY, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Thank you, Chairman Connolly.

Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you for the opportunity to testify on the FITARA scorecard.

For the past three years, I have worked for MITRE, a not-for-profit corporation that operates in the public interest. Currently, I lead its Center for Data-Driven Policy where we connect our expertise on topics like acquisition and cybersecurity to policymakers in both the legislative and executive branches.

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 testified at the first six scorecard hearings and again at number 10.

I have two overarching points to make this morning, Mr. Chairman. First, the scorecard has resulted in significant improvements to Federal IT management, and second, we need to get similar results in additional areas by updating the scorecard.

Chairman Connolly, I would like to thank you for your leadership along the way not only in creating FITARA but also with your unprecedented follow-through with nearly seven years of consistent oversight.

The Federal IT community has benefited greatly from working with you and your bipartisan partners along the way—Representative Issa, Hurd, Kelly, Meadows, and now Ranking Member Hice. The progress that has resulted from the scorecard and your oversight is significant. Here are a few highlights.

There have been billions of dollars saved on consolidating data centers and duplicative business systems. Regarding acquisitions, agencies now acknowledge and manage risk better and deliver in smaller increments.

And the CIO role has really elevated. CIOs who are involved more in the budgeting and procurement processes and more have a seat at the executive table.

But now is the time to update the scorecard to get similar results on more pressing IT and cyber challenges confronting agencies. Currently, the scorecard has seven areas that are graded. Three should be retired: incremental, portfolio stat, and data sets.

The remaining four should be incorporated within one of the five categories that I am proposing today. Those five categories are cybersecurity, work force, legacy modernization, budgeting, and infrastructure. Here is a brief rundown of the five.

Consistent with your comments, Ranking Member Hice, we need to update the cyber area by using metrics that are consistent with the administration's cyber executive order, its zero-trust policy, supply chain risk management best practices, and those metrics used by CISA in the industry.

These metrics should be consistent with the revisions this committee is considering to the Federal Information Security Management Act, or FISMA.

Second, we need to add an IT and cyber work force category that provides a comprehensive view of agencies' gaps in critical IT and cyber areas that tracks progress to build the appropriately skilled work force. It is critical here that CIOs work closely with their agency's chief human capital officers.

Third, we need to 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.

My written statement provides details like using the IT dashboard to track progress on these acquisitions and having OMB play a prominent role in ensuring progress. Not addressing these legacy systems will hinder the administration's ability to make the desired progress on customer experience and zero-trust, which are both administration priorities.

Fourth, we need to add an infrastructure category that will continue to shine the spotlight on having modern and secure networks with the EIS contract but should also include, Mr. Chairman, a cloud-adoption metric and move on from a data center focus.

And No. 5, we should add an IT budgeting category that continues the pressure on establishing working capital funds but also incorporates technology business management so that IT costs are better captured. We need to shed light on the discipline agencies use in budgeting for IT so that it reflects actual agency needs for modernization.

One final point before I wrap up. It is critical that the updates to the scorecard are coordinated with the Federal CIO and OMB since they have been and will be the source of most of the data used in the grading process. In fact, as GAO's testimony highlights, five of the seven areas currently graded rely on OMB data.

In summary, Mr. Chairman, these five recs are about having better secured agencies, tackling true mission enhancements, having a modern infrastructure, a skilled work force, and the right resources.

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

Mr. Chairman and Ranking Member Hice, we look forward to further working with you so that our Federal Government has the right focus, transparency, and measurement to secure and advance agency missions.

This concludes my statement. I look forward to your questions.

Mr. CONNOLLY. Thank you, Mr. Powner, and it is very helpful to hear your thoughts since you helped design the original scorecard about what we need to do to update that scorecard to make sure it is relevant in capturing the relevant information.

Suzette Kent, another friend and familiar face, welcome back.

STATEMENT OF SUZETTE KENT, CEO, KENT ADVISORY SERVICES, FORMER FEDERAL CHIEF INFORMATION OFFICER

Ms. KENT. Thank you, sir.

Chairman Connolly, Ranking Member Hice, and honorable members of the subcommittee, thank you for inviting me to be part of the discussion today on evolving the Federal Information Technology Acquisition Reform Act.

I last appeared before this committee when serving as the Federal CIO, and today I am talking to you as a technology and transformation business executive working with both public and private sector companies around the world, and I am here with enthusiasm.

It has been a great, great conversation to start off, and it is very important when congressional leaders dedicate their time and attention to improving the ways that Federal technology serves citizens and helps us deliver on agency mission.

My comments today are going to center on two areas: evolving what is measured and maybe innovating on how those things might be measured.

I support a scorecard that brings visibility to the results achieved and coalesces the focus between the people doing the work and the people who approve the funding, and I applaud the accomplishment since the inception of the scorecard and, like this committee, I endeavor for the scorecard to be something that really matters to agency leaders and is helpful to the CIOs and their teams.

It is a great achievement when agencies meet the targeted goals and we have seen that, but it is also a celebration when a category can be removed because it is an opportunity to introduce new metrics that are focused on future expectations, and in this way the FITARA scorecard continues its legacy of driving focus on forward progress that your constituents expect.

The scorecard has served as a mechanism to drive that continuous improvement. You have heard that already from multiple witnesses.

But we are also in a new era. Federal technology is the engine for how remote work is done by our Federal work force, and digital and mobile channels are now the primary engagement platform that most Americans use for critical government functions.

Inside government we have important goals reflected right now in law and policy, laws like the 21st Century IDEA Act, evidence-

based policymaking. We have executive orders on cybersecurity, customer experience in AI, and we have the president's management agenda themes and a Federal data strategy that span multiple administrations and take a bipartisan approach to accomplishment.

Yet, the objectives that are defined in these aren't in the scorecard yet. So, to maintain the impact of the FITARA process, there are four areas that I would, humbly, submit to this committee for future consideration. Some of these things are going to seem familiar.

No. 1, cybersecurity. Last week's FISMA discussion covered many of the key points. But future scorecards could drive how we make cyber metrics more timely and reflective of the current threat environment.

Also, allow us to address the risks in our changing operating environment including identity and access protocols and accelerating information sharing, as the EOs point out.

Modernization, second. It never stops, and we know that evolution of legacy technology, digital capability development, advancing our disciplines around data, and expanded use of automated technologies are all part of that modernization effort.

That continuous modernization also demands changes to some of the rigid funding and procurement processes to better align with multi-year initiatives and best practices for modern technologies, the types of things that you have embedded into the goals for working capital.

I am also going to call out as the third point digital. Although digital journey is part of modernization, it deserves some specific near-term attention because your constituents are so digitally dependent.

Now is the time to include metrics that highlight our progress toward digital and mobile native platforms, quality customer experiences that are on par with what citizens' experience in every other industry, and we have goals that are already defined both in law and the EOs that could be elevated for incorporation into that future scorecard.

And the fourth is work force. We have an opportunity to signal priority and investment in our most precious resource in all of Federal IT, the people. Metrics to ensure that priority is given to skills development and work force performance should be included because, as we are evolving the technology ecosystem, we cannot under invest in our Federal work force.

And now, quickly, for the how we measure. As I return to the private sector, I often see that citizens judge their experiences with government using the same lens as their private sector businesses, but they can't take their business elsewhere.

Maybe we could consider leveraging some external metrics as well that are widely accepted across other industries that have long histories. There are CX metrics, cyber scorecards, and even people measures that could help those inside government more objectively see how they are perceived by citizens and accelerate some of our path forward.

Government may never be as leading edge as private sector. But as you have stated, we can show meaningful year over year improvements that matter.

I applaud the committee's attention to Federal technology matters. I appreciate your focus on ways that we continue to leverage this success to move forward and to continue to drive improved outcomes.

Thank you for including Mr. Powner, Mr. Spires, and I in this dialog, and I look forward to answering your questions.

Mr. CONNOLLY. Thank you so much, Ms. Kent, and very thoughtful. We really appreciate it.

And last but not least—again, a familiar face, an old friend—Richard Spires?

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

Mr. SPIRES. Thank you, Chairman Connolly, and good morning to you and Ranking Member Hice and members of the subcommittee. I am honored today to testify in regards to the FITARA and the FITARA scorecard.

While the FITARA legislation itself has been an aid to agencies, I believe it has been the oversight of Congress that has been a driving factor in getting agencies to improve their IT management.

In particular, the spirit of bipartisanship of this subcommittee on Federal IT issues has made a very positive difference. Yet, even with the progress, much work remains to reach a state of IT management best practice.

In 2015, the GAO placed the whole Federal Government on its high-risk list for improving the management of IT acquisitions and operations.

In its latest report published in March 2021, GAO states that the government has only partially met requirements in four of the five criteria related to the elements of this high-risk item, and it is disappointing that the ratings for all five criteria for this high-risk item did not improve over the past two years.

The FITARA scorecard has been effective in helping drive successes in the areas of data center consolidation, software licensing, and the use of incremental delivery methods.

Now is the time to substantively evolve the scorecard to address the core IT modernization challenges agencies face, as highlighted by GAO's audit work following our four recommendations that can have a significant near-term impact on agencies' abilities to drive successful IT modernization.

The first one, add an IT planning category. Meaningful IT modernization starts with good planning. Hence, this category should reflect the maturity and focus on IT modernization within the agency's planning function and enterprise architecture.

To measure this category, existing best practices for planning and managing IT could be used either by GAO or agency IGs to audit an agency's IT planning capability to arrive at an IT planning maturity grade.

Recommendation two—combine the incremental delivery and transparency in risk management categories under 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 to manage such programs.

There are well understood and documented best practices that can be measured to arrive at a composite grade for this particular category.

Recommendation three—evolve the managing government technology category to a broader IT budget category. This category should use the technology business management—TBM—taxonomy so agencies better understand the cost elements of their IT budgets.

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

And finally, not surprisingly, evolve the cybersecurity category. This category does need to be revisited. The existing FISMA measures and cybersecurity cap goals do not accurately measure an agency's cybersecurity posture.

The good news is that the recent executive order on cybersecurity issued in May 2021 can serve as a blueprint for what Federal agencies should be doing to enhance their cybersecurity position.

In particular, the EO places special emphasis on agencies implementing a zero-trust architecture, having holistic visibility across one's IT infrastructure, implementing secure guidelines in cloud-computing environments, focusing on protecting high-value data and system assets, and dealing with supply chain issues. The EO can serve as a means to more accurately grade an agency's cybersecurity posture.

To determine the specific measures for a category and what additional data would be required so that the category could be properly graded, Congress should 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.

Mr. CONNOLLY. Mr. Spires, we are going to—if you could wrap up because——

Mr. SPIRES. Yes.

Mr. CONNOLLY. Thank you.

Mr. SPIRES. OK. I think I have made my key remarks. So, thank you for the opportunity to testify.

Mr. CONNOLLY. Thank you, and we will have an opportunity to explore even further, of course, in questioning. Thank you so much.

Mr. SPIRES. Sure.

Mr. CONNOLLY. The chair now recognizes Mr. Khanna of California for his round of questioning, and I thank Ms. Norton for yielding.

Mr. KHANNA. Thank you. Thank you, Chair Connolly. Thank you, Ms. Norton, for giving me the opportunity.

I want to thank both the majority and minority staff for working with Nancy Mace and me on a bill to ensure that our Federal Government is prepared to tackle the powerful quantum computing challenges.

In the future, the challenge is what if people are able to break encryption, and even though classical computers can't break encryption now, our adversaries can steal our data in the hopes of decrypting it later.

It is my belief that the Federal Government needs to think about how to move our encrypted data to algorithms that use post-quantum cryptography, and I have been working, like I said, with Representative Mace and with great input from both the majority and minority staff in helping us craft this.

NIST, as you know, is working on new standards, which should be finalized by 2024. I had a few questions for Ms. Ann Dunkin. What are you doing now to address this threat and what do you think Congress should do?

Ms. DUNKIN. Representative Khanna, thank you for asking about quantum computing. Quantum encryption is an area of great concern to us in the Federal Government.

As my role as chair of the Innovation Committee as part of the CIO Council, we have been addressing quantum computing and quantum encryption and raising visibility within the community across the government among CIOs.

We are—have a two-pronged approach, I think, to this issue. One is that, as you know, there is a risk that data can be exfiltrated now and then decrypted later, and so we are emphasizing securing data and trying to ensure that we do not lose data now that could be decrypted later.

In addition, we are working with NIST and across the DOE enterprise to understand and develop quantum-resistant encryption so that, going forward, we will be able to protect Federal data from quantum computers when they are eventually in the mainstream.

Mr. KHANNA. Thank you very much for that.

Ms. Harris, do you think we should begin to strategize—study this change and do you know how much it would cost or how we should prepare for this?

Ms. HARRIS. Thank you for the question.

We issued a study on the status and the prospects of quantum computing and communications. I do think that we do need to do more work in this area as the Federal Government. In that report, we present four major policy options and potential implementation approaches.

But, basically, it covers how to address the collaboration across industries and disciplines as well as countries in developing quantum technologies.

It also discusses ways to expand the quantum work force, how to incentivize or support investments in quantum technology, as well as the need to develop a robust and secure quantum supply chain.

So, those are areas that we have begun to dive into, and we are happy to work with you on these policy options and the best approaches to implementing them.

Mr. KHANNA. And I appreciate that, and I am familiar with your reports and look forward to working on what more needs to be done.

Ms. Dunkin, if I could ask you one more question. Do you know which systems at your agency can or cannot be moved over to post-quantum cryptography?

Ms. DUNKIN. Representative Khanna, thank you for that question. That is not a question I can answer today. We would be happy to look into that. It is a fairly large lift to identify that, but we would be happy to do some research and get back to you.

Mr. KHANNA. Terrific. And one more question either for you or for Ms. Harris. When should we begin to migrate our data over to post-quantum cryptography? Is now too soon or can we do it—start to do it now?

Ms. DUNKIN. I think, Representative, as soon as we are able to identify algorithms that will allow us to have quantum-resistant encryption that we can and should begin to move to those solutions.

Mr. KHANNA. Well, I appreciate it. I appreciate the expert testimony.

Let me just say, Mr. Chair, that I am appreciative, again, of Representative Mace working on this and the excellent input from majority staff and minority staff, and look forward to working with you and our witnesses and the committee staff on this legislation.

Mr. CONNOLLY. Thank you, Mr. Khanna, and I look forward to working with you and Ms. Mace on your legislation as well.

The chair now recognizes the ranking member, Mr. Hice, for his round of questioning.

Mr. HICE. Thank you very much, Mr. Chairman. I will try to go quickly, and if the panelists—if we could try to answer quickly. I want to get as many other members on here as well.

Ms. Harris, let me start with you. I mentioned a little while ago in my opening statement that in the FISMA hearing last week I asked the GAO witness whether the FITARA metrics gives an accurate picture of the agency's security posture and, of course, the answer was no.

So, my question to you, real quickly, can you give some specific suggestions that this committee needs to just get a better assessment on the issue of cybersecurity?

Ms. HARRIS. Sure. So, I think that is—as Mr. Spires and Mr. Powner had identified, I think using the administration's executive order on cyber as a basis for how we take a look at evolving the cyber metric, I think that is a good idea.

In terms of what is currently not captured in the current metric, IT supply chain is one example. We have done work for you very recently to take a look at that pulse check across the Federal Government.

So, we have work that can support either evolving the metric to expand into supply chain as well as on, you know, expanding to take a look at more enterprise-wide cyber initiatives. You know, we have ongoing and recent work that we could, certainly, support in those areas.

Mr. HICE. Regarding the Enterprise Information Solution metric, 15 out of 24, as already been mentioned today, are failing. Do you have any thoughts as to why these grades are so low in so many agencies and what needs to happen to get back on track?

Ms. HARRIS. Yes. So, I think similar to what occurred with software licensing, it just wasn't a top priority for the agencies.

When you take a look at the history of the past two telecommunication transitions, agencies have sort of drug their feet in this initiative and, really, did not make it a priority until they were close—very, very close to the deadlines for closing out those current set of contracts.

So, I applaud this subcommittee for including EIS as part of the scorecard and we need to just continue to push and put the heat on the agencies to make it a priority.

Mr. HICE. OK.

Mr. Spires, let me hit you, real quickly, in the context of evolving the cybersecurity category. You stated in your testimony, quote, "Agencies should emphasize effectively measuring cybersecurity risks associated with cloud development and moving beyond static compliance-based checklists." How do we do that?

Mr. SPIRES. Well, thank you for that question, sir. There are, absolutely, numerous tools now available from companies—product companies—that can do more real-time monitoring of what is going on in the cybersecurity environment.

And let me just say, one of the big problems we had with FISMA and, you know, the law was originally—in the early 2000's past, you know, we got into a bit of a compliance kind of checklist mentality and we just need to move beyond that. Things are moving so quickly. Your cybersecurity posture is changing so rapidly. You need to be able to use automated tools to be able to help measure that.

Mr. HICE. OK. Very good. Final question.

Ms. Kent, you had mentioned that—well, one thing that I have brought up several times on these scorecard hearings is the need to gauge customer satisfaction, and you had mentioned that we need some metrics to go across other industries—I am assuming private sector and so forth.

So, can you expand on this a little bit as to how we might adopt some of these metrics in our government?

Ms. KENT. Certainly. Thank you for that question. We already have pieces around websites being mobile friendly, 508 compliant.

Do they have data-driven functionality? Do we have secure connections? Kind of goes to some of the questions that already have been asked.

Those are things that we might consider, you know, in the near term and, in fact, some agencies, because they have been part of law, have already started tracking those themselves.

Specific, you know, as we look at common measures across industry's ease of use, and that is something that is pointed out in the EO, and then how effective they are for the intended service they are delivering, whether it is information or, you know, a payment or some type of process.

Those types of things are in motion, and we could measure those very quickly, and in those areas there is metrics that are already both in government and then widely used outside, and they are meaningful to constituents.

Mr. HICE. Very good.

Mr. Chairman, we have got some other questions that we will submit but I want to yield back to other members, and thank you for this hearing, again.

Mr. CONNOLLY. Thank you, Mr. Hice.

And, Mr. Hice, I just want to underscore something Mr. Spires said in response to you, which is, like FISMA, we have got to really be careful about what metrics we set.

So, for example, you can set a metric in terms of everybody has to be educated and made aware and everyone goes through a training course, and that is a metric I can easily meet and I check that box.

Meanwhile, the real goal—that is only a—that is a means to an end, not an end in itself, right. The goal here is to make ourselves cyber secure and, meanwhile, you know, hackings go up, but we are educating everybody.

So, I think as we look toward our FISMA legislation, you and I want to be really mindful of avoiding those traps, and I think Mr. Spires advises us well with respect to that. Thank you.

The distinguished Congresswoman from the District of Columbia—and thank you for your willingness to yield to Mr. Khanna—Eleanor Holmes Norton?

Ms. NORTON. Of course, Mr. Chair, and I very much appreciate these biennial hearings because implementing FITARA and other IT laws leads to improved use of IT acquisition practices that will help—that will have ripple effects throughout the agencies and then, of course, across the Federal enterprises.

Yet, in some cases, technology has outpaced existing laws and administrative guidance. Agencies' performance on the FITARA score side has plateaued.

While the December 2021 scorecard resulted in a 53 percent—in 53 percent of agency grades unchanged, the July 2021 scorecard resulted in a record 75. That is, 75 percent of unchanged grades.

Ms. Harris, what is causing a plateau in agency progress on the scorecard?

Ms. HARRIS. I think, in part, it is the methodologies that we use for—in at least two of the categories, which were grading on a curve.

So, agencies are less motivated to strive for continued risk management transparency and portfolio stat savings when they don't believe that they can reach, you know, the best possible grade in those categories.

So, I think that the change in the methodology in which we go about those two categories, if those categories still remain, is very important to ensuring that agencies continue to strive in those areas and not plateau.

Ms. NORTON. Ms. Dunkin and Mr. Cavallo, with the exception of OPM's most recent grade, both of your agencies have maintained on average a C+ grade on the scorecard. Is this an accurate picture of your agencies' IT management progress? Why or perhaps, why not?

Ms. DUNKIN. Representative Norton, thank you for that question.

Yes, I am—I would say that it is a mixed picture as to whether those metrics are accurate representations of DOE's progress. I

think there are definitely places where the metrics reflect the need for improvement.

Like, there are a couple metrics, or at least one metric, where it is not an accurate reflection of DOE's performance and where DOE is doing a bit better and that is in security where there is a lot of consolidation of metrics in their pass/fail.

So, I think we are doing a little better in security than it might look. I think a lot of this is fairly accurate. I think that other folks who have talked today have mentioned the metrics that are on a curve, and those make it challenging. If you can't move up in your peer group, you are going to get stuck. So, I think it is a mixed bag and we definitely have work to do with you, and we are going to continue to do that work.

Mr. CAVALLO. Thank you, Congresswoman, for that followup question. Again, I was pleased to see that we did move up a full letter grade in the scorecard.

But like Ms. Dunkin said, it is not a total accurate picture because so many of the measures are difficult to nail down. I definitely see us making progress at OPM as reflected by that improved score, and even the scores that we haven't improved in the time since I have been here, I see us taking concrete steps that maybe haven't been enough to trigger us up to the next grade. But we are headed on the right path.

I think on the panel we have heard a number of great suggestions today of possible other ways to expand the scorecard. But I do want—I commend the use of the scorecard.

I think it is critical for us to have a common measure across the Federal Government, and I know I am very interested in working with—Ann and I are both on the Innovation Committee of the CIO Council. Definitely, it is hard to measure everything perfectly.

We will be very happy to help participate on possibly changing some of those metrics, again, as the chairman started off the hearing, not for us to just get a checkmark and get a gold star, but to actually modernize the entire Federal Government.

Ms. NORTON. I would like to get this question in from all of the witnesses before my time is out. For all of you, how does the timing of the scorecard cycle impact the accuracy of grades and the ability to demonstrate meaningful change at agencies?

I would like that answer from all of you. Timing.

Ms. HARRIS. I think that looking at the cadence of the scorecard is something that we should take a look at, and we are happy to work with you and the subcommittee on that.

I think that, in some cases, the data can be stale because of the timing of the scorecard, and then in other cases, you know, we are having to collect information manually from the agencies in order to populate the grades.

And so that is something that is quite time consuming and is—you know, given that these scorecards are issued in six-month cycles, it is a challenge, I think, for some agencies to be able to demonstrate progress in that—in those short periods of time.

So, we are very open to taking a look at the cadence of the scorecard for sure.

Mr. SPIRES. In my——

Ms. NORTON. Yes?

Mr. SPIRES. In my written testimony, I noted that a couple of the measures I am recommending are a little more complex, such as an ability for an agency to deliver IT programs and how mature they are in that, and I think such a measure would require an audit from, like, the agency IG.

So, I would be recommending that for that particular measure, if that were to be adopted as an example, that might be something you would do yearly. That does not mean you couldn't have an update every six months and there, certainly, are measures, I think, that lend themselves to every six months.

But I think as you look at trying to drive measures that are around modernization, for instance, there are, perhaps, more complex measures that would require more time and also give agencies more time to, if you will, improve, because six months is such a short time cycle for an agency to make real change.

Ms. NORTON. Any of the rest of you have any answers on that question?

Mr. POWNER. Yes. Congresswoman Norton, I would just—I would second that. I think initially when the scorecard was developed it was very important to have a six-month cadence because the message was the committee was very serious about this and we were going to do it with this great frequency. I think the complexity of some of these new metrics that we are considering an annual cycle would be just fine.

Ms. KENT. Congresswoman Norton, thank you for your question. I would add that you heard many of the speakers talk about automating metrics, places where we can both introduce new metrics and automate those, you know, help the reporting be more timely and transparent.

And, you know, to Mr. Powner's point, the—it is important that results from the scorecard and progress or lack thereof and important issues can inform both budgeting and priority processes as well.

So, that cadence is important for congressional members to see what agencies—you know, what results they are delivering and have opportunity to take action through other processes where you support either funding or inform other needed pieces of law.

Ms. DUNKIN. Representative Norton, I would just add, I think that there are some metrics that we are talking about and that exist that are very complex and time consuming and would be better on an annual cycle.

As Ms. Kent mentions, we may be able to automate those metrics. You might be able to generate a hybrid scorecard where some metrics come out twice a year and others only come out once a year.

Ms. NORTON. If I have any more time, I have another question for Ms. Harris. Given the——

Mr. CONNOLLY. Actually, I am afraid we have gone over time, and because of my desire to accommodate everyone before, you know, the hammer drops——

Ms. NORTON. Of course.

Mr. CONNOLLY [continuing]. but we—if we have more time, Ms. Norton, maybe we can return.

Ms. NORTON. Thank you.

Mr. CONNOLLY. Thank you, ma'am.

The distinguished gentleman from Pennsylvania, Mr. Keller, is represented for his round of questioning.

Mr. KELLER. Thank you, Chairman Connolly, Ranking Member Hice, and I want to thank our witnesses for participating in today's hearing.

The FITARA scorecard remains a valuable tool to help modernize the Federal Government's IT systems in cybersecurity infrastructure.

Strengthening our Nation's IT infrastructure and cyber grid is a goal all Federal agencies must work toward. The Federal Government spends, roughly, $100 billion on cybersecurity and IT investments each year.

Yet, we still face challenges securing some of our Nation's most sensitive IT systems. These challenges have been highlighted by events such as the Colonial Pipeline and SolarWinds cyber-attacks.

Congress and the administration must now look to cost-effective strategies to improve our Nation's IT system and cyber readiness.

A reoccurring problem for veterans across the country is the reduced operation of the National Personnel Records Center, which is responsible for providing veterans access to documentation required to receive certain VA benefits.

The NPRC has accumulated a backlog of more than half a million vital information requests from veterans and their families, some of whom have waited for over a year for their documents. The NPRC has indicated an ongoing effort to digitize its current system of physical records.

My question would be for Ms. Kent. With reduced personnel onsite at the NPRC in St. Louis, how do we quickly and responsibly digitize these records to make them more easily accessible while ensuring this information remains secure and protected from a variety of cybersecurity threats?

Ms. KENT. Congressman Keller, I have not been deeply involved in those sets of activities. But as we have touched on, there are many of the automated technologies that we can leverage to digitize records that, by nature of using that technology, helps us secure the information better and makes it more widely available to other systems.

And as we talked about, you know, security, it is both the technology as well as the data in its raw form, and in that particular situation there is a significant volume, as you mentioned, that is still in paper form, so it is not readily available to support veterans and the needs of their family, and as the wife of a veteran I understand that situation very keenly.

So, I think we strongly encourage leveraging those automated technologies and freeing the data to allow quicker, more timely, and less error-prone servicing.

Mr. KELLER. Is there anything Congress can do to help move that along?

Ms. KENT. When we talk about some of the individual metrics and things like that, there are opportunities to look at and measure as part of legacy activities reliance on paper-based records and how information is provided, and there is elements in the Federal data strategy that talk about digitizing information or making in-

formation available for broader use, and those might be some of the elements that we would be happy to talk about, you know, in committee where having them tracked on a scorecard would benefit not only this purpose but any agency that has a significant amount of paper records.

Mr. KELLER. Thank you. I appreciate that.

Mr. Spires, the Enterprise Infrastructure Solutions contract is a massive $50 billion contract intended to modernize agency network infrastructure.

However, I have concerns regarding this high price tag when a thirteenth FITARA metric—the thirteenth FITARA metric has identified many more failing grades for agencies compared to the last scorecard.

Can you speak to the reasons for these failed grades and how we can move toward a more, you know, a more accurate or better system?

Mr. SPIRES. Thank you, sir. Yes, my experience and it even goes back to the—when we did this last migration to the networks contract and now we are moving from networks to the EIS—you know, it is—I think, you know, many agencies struggle and it was brought up by a couple of the panelists here that the work force issues that we face within Federal IT.

You know, many of the OCIO organizations do not have all of the talent that they need to effectively manage their IT, and that is one of the key issues that we face in Federal IT and it manifests itself in many ways.

But one of those is in this example. You know, it is a significant undertaking to migrate from one major networking contract to another and it takes a lot of work behind the scenes within these agencies to make that happen, and I think many agencies struggle with that while they are also dealing with the day-to-day operations and trying to modernize some applications and the cybersecurity issues. You know, the work force issues, I think, are all—are really behind a lot of where we see struggles with these types of operations.

Mr. KELLER. You mentioned something about not having the talent. I mean, that is concerning, and I am wondering what we need to do to make sure that we have the talent necessary.

I mean, that is what every American should expect our government to be able to do. So, what do we do to make sure that we get the talent to be able to handle these things?

Mr. SPIRES. Yes, that is a great question and a key question that many of us have been facing for decades, how do we up-skill—I mean, get—you know, we have great people in government. Don't get me wrong. It is an amazing set of people.

But on the other hand, to your point, we have real talent gaps, particularly in the technology areas and be able to manage a lot of these technologies, and I think we have to really do look at that.

And, you know, others have said, hey, there is an area in the scorecard, that perhaps we should add a category around this whole issue of the talent—the IT talent within the——

Mr. KELLER. Well, I guess I would say that wasn't actually my point. I heard you say that and that is what brought the concern up. So, I wasn't—that wasn't my point. I wouldn't know that, not

being in that realm. But if that is something that you need to look at, I think we should support that.

Thank you, and I yield back.

Mr. CONNOLLY. Thank you, Mr. Keller. And by the way, one answer to your question is support my Federal internship bill so that we can try to make sure we are recruiting the skill sets of the future that we desperately need, and I look forward to trying to work with you on that.

Votes have been called. We have two more members to be heard. Pleased to recognize now our newest member but our most faithful already, the distinguished gentlelady from Ohio, Shontel Brown.

Representative Shontel Brown?

Ms. BROWN. Thank you, Chairman Connolly and Ranking Member Hice, for holding a hearing on FITARA today, and thank you to all the witnesses for joining us.

As we heard last week during the FISMA reform hearing, technology is ever changing and this is why we need periodically to update critical IT laws that will modernize Federal technology, strengthen Federal cybersecurity, and improve the operations of the Federal Government.

So, my question is for Ms. Harris. The Federal Government has projected that it will spend approximately $111 billion on IT investments in the Fiscal Year 2022. Of the $111 billion, 57 percent—roughly, $63 billion of it—will be spent on operations and maintenance of existing systems and about 15 percent, which is about $16 million of it, will be spent on development, modernization, and enhancement.

Could you describe the difference between these two categories of IT investment?

Ms. HARRIS. Sure. So, with the operation and management or—and maintenance—the O&M dollars—that is spent toward sustaining systems and, in particular, we have a major legacy IT issue in the Federal Government.

And so, a large portion of those O&M dollars are spent toward unsecure and unstable systems that we need to tackle that issue. The development, modernization, and enhancement—DME dollars—goes toward investments in new and developing newer modern systems.

And so, what we want to see is more of those O&M—we want to see decommissioning of those legacy systems so we free up those dollars to be able to spend in the DME category.

So, that is really the goal here, and we really need to be very focused on tackling that legacy issue because that spans not just a management issue but a cybersecurity challenge as well.

Ms. BROWN. So, Ms. Harris, how might we use the scorecard to incentivize the agency to invest more in the IT modernization?

Ms. HARRIS. I think one thing we should be doing is, potentially, adding a category that is focused on the legacy IT issue and I think that there are a number of ways that we can address that issue.

But, perhaps, one of those is identifying the most critical legacy systems across the Federal Government within these agencies and then tracking the progress in decommissioning those systems, and that might be a potential way to track the legacy issue and be able

to, you know, push the Federal Government into more modern technologies and modern systems.

Ms. BROWN. OK. Thank you very much.

My next question is for Mr. Cavallo. To effectively modernize and acquire nimble technology we must work to fill the skills gap in Federal IT and cyber work force.

Unfortunately, GAO has reported that the skills gap in IT and cyber positions across the Federal Government are contributing to significant IT management and the acquisition challenges.

Can you and Ms. Dunkin describe how incorporating the skills gap analysis into IT and—into your IT and cyber work force plans?

Mr. CAVALLO. Thank you, Congresswoman, for that important question. We have heard from the other panelists how difficult it is to make sure that we have the current updated skill sets in today's government work force.

What I found in my career, by providing the latest in technologies such as cloud technologies is the best way for us to attract early career talent.

The chairman talked about his internship program. We have to push every lever that we can to get today's work force interested in working in the Federal Government.

At OPM, one of the things that I have done to help retain the staff, because not only do we have to hire them but we want them to stay in government, is to implement an extensive training program and a certification program that either matches or exceeds what a lot of private sector companies do.

So, I think, you know, giving a great work environment with the right technologies is one of the ways that we can solve that problem, and as I highlighted in my oral statement, I have been able to close our vacancy gap considerably. So, those steps that I am taking are working.

Ms. BROWN. Ms. Dunkin?

Ms. DUNKIN. Thank you, Representative Brown.

Yes, so we are doing a number of things at DOE to try and close that gap. But what I am most excited about is the internship program that we have put in place.

We call it our Omni internship program, and this summer we will have 200 students from overburdened and underserved communities coming out to our DOE sites and plants across the Nation in cohorts.

So, No. 1, we are paying these students. The government often offers unpaid internships. These are paid internships. And second of all, we are providing the support to get them to our often-remote locations.

So, we are ensuring they have transportation, we are ensuring they have housing, and we are making sure that they are part of a cohort so they will carry their experience on, and then we are going to bring those same students back to other departments, other parts of the department, each summer so they get a whole view of DOE and, hopefully, we will turn those into Federal employees, going forward. So, that is the first thing we are doing.

Second, we use all the flexibilities we have because not only is it hard to attract folks to the government, but it is a slow process. And so when we can use flexibilities like direct hiring, we can

bring people in quickly and not lose those folks to the private sector that has a faster process.

We are also looking—yes?

Mr. CONNOLLY. I am sorry. Go ahead. Wrap up and——

Ms. DUNKIN. Yes. We are also looking at our flexibilities around pay. That was the last thing I was going to say, Chairman. Thank you.

Ms. BROWN. And my time has expired. Thank you. Thank you, Mr. Chairman. Thank you, Ms. Dunkin.

Mr. CONNOLLY. Thank you, Congresswoman Brown, and sorry to interrupt you, Ms. Dunkin. I didn't mean to do that.

Congressman Clyde, are you there?

[No response.]

Mr. CONNOLLY. We will return to Mr. Clyde.

Mr. Lynch, welcome. The distinguished gentleman from my hometown of Boston is recognized for his line of questioning.

Mr. LYNCH. Well, thank you, Mr. Chairman, and you and I know we have been working on this issue for a long, long time. We have been talking about these legacy systems for 20 years, and looking at the scorecard, many of these agencies have not improved much.

Ms. Dunkin, the Department of Energy received a D grade in cybersecurity and, notably, your agency has met none of its cross-agency priority goals on cybersecurity.

Similarly, OPM has had a very difficult history on cybersecurity. We have had some embarrassing vulnerabilities there and breaches.

Let me ask you—I don't even know where to begin. This has been such a disappointment. You know, we in government try to encourage the private sector to be more careful with the data of our constituents and, yet, the government itself seems to be the epicenter of vulnerability for much of the important information that we are custodians of in government.

Can I ask you, Ms. Dunkin, we are dealing with this Log4j vulnerability now with a system that was already vulnerable, and now with the Log4j vulnerability on top of that be so ubiquitous, how are we dealing with fixing that vulnerability in the face of the dangers that it represents?

Ms. DUNKIN. Representative Lynch, thank you for that question. We are addressing Log4j with great expediency. We identified the systems within DOE that have potential vulnerabilities and we have gone through and remediated those.

All of department elements, including all of our national labs, have reported their results and are either completed in those—in remediated vulnerabilities or nearing completion of remediating those.

With Log4j one thing we know is that we don't necessarily know the entire landscape of potential vulnerabilities.

So, we will continue to be vigilant and aware, and as new vulnerabilities are identified we will continue to patch those. We do have a very robust process within DOE to ensure that we complete that process, and we are working through it.

Mr. LYNCH. I got to admit, I think that is happy talk. That is happy talk.

When I talk to the cybersecurity people, you know—and I have the wonderful pleasure of chairing the National Security Subcommittee, and we have received classified briefings on this—and that is not—that is not what people are saying.

They are saying Log4j goes back to these legacy systems, and it is so ubiquitous and so difficult that we are going to be at this for a long, long time just on that one vulnerability.

So, Mr. Cavallo, what is your approach in terms of—and where do you think we stand in terms of responding to this Log4j vulnerability and how long do you think it is going to take us to clean that up?

Mr. CAVALLO. Yes. Thank you, Congressman, for that question, and I do want to assure you that at OPM we consider—I used to chair cybersecurity posture for all of our information systems. It is a top priority for us. As Ms. Dunkin highlighted and you have highlighted yourself, this is a very broad and extensive risk availability.

What I would, respectfully, like to request is that I will be happy to followup in a more secure setting with our exact status of where we are on that.

Mr. LYNCH. Yes, that is a reasonable request and I am happy to do that.

As a matter of fact, Mr. Chairman, we might want to—and Ranking Member Hice, we might want to do a classified in order to really dig down on some of these vulnerability issues and where we are on this, and I agree with the gentlemen it might be better to take place in a secured setting.

So, with that, I appreciate your attention to this issue. I appreciate your good work, and this is one of those issues that is, truly, of a bipartisan concern.

So, with that, I will yield back the balance of my time. Thank you.

Mr. CONNOLLY. Thank you, Mr. Lynch, and we can—absolutely, our two subcommittees could collaborate on that classified briefing. We will, certainly, defer to your subcommittee on that matter and be glad to cooperate. So, thank you for your leadership.

I see Mr. Clyde. The gentleman from Georgia has returned. So, Mr. Clyde, you are recognized for your—on your questioning.

Mr. CLYDE. Thank you, Mr. Chairman. I appreciate that and I appreciate holding this very important hearing.

This question, ma'am, for Ann Dunkin of the Department of Energy.

Ma'am, in your testimony here you say FITARA helps to ensure the Department of Energy's IT and cybersecurity programs are strong enough to support and enable the vital work of the department across the three main priorities set by the secretary: combating climate crisis, creating clean energy union jobs—and that is not jobs, that is union jobs—and promoting energy justice.

Now, you know, I thought the Department of Energy was responsible for the security of weapons-grade nuclear material, and these are your three top priorities.

Promoting energy justice—what is that?

Ms. DUNKIN. So, Representative Clyde, thank you for the question. Energy justice reflects the president's priority to ensure that

the benefits of our investments in energy accrue at least in part to underserved and overburdened communities, sir.

Mr. CLYDE. So, I didn't know that justice—or that energy needed justice. You know, I mean, if the department would spend a little bit more time on maybe the things that are more important—I understand that your agency received a D for—grade for FISMA—the FISMA category.

So, has your department's performance or lack of performance in this area in any way exposed any United States infrastructure, national security sites, or any soft or hard targets to cyber-attacks?

Ms. DUNKIN. Representative Clyde, I think that is a conversation that I would also suggest should happen in a classified environment.

I would be more than happy to talk to you about the specifics of the DOE's security posture in that kind of environment. Rest assured that we are vigilant in ensuring the security of DOE's assets and—but, again, any specific issues we will want to take to a classified environment.

Mr. CLYDE. Well, you know, with a grade of D, that doesn't give me a whole lot of confidence. You know, I think that the Department of Energy's priorities are a little misguided here. I just read those three priorities that you have and, obviously, one of them is not FISMA.

Ms. DUNKIN. So, Representative Clyde, thank you for pointing that out. Those are the secretary's priorities. Rest assured that within the secretary's priorities and my priorities, cybersecurity—FISMA—are very high priority.

We are—we believe that our security posture is stronger than the FISMA goals—the FISMA score reflects and you will start to see over the next few months in the quarterly reports improvements in those metrics as we implement some specific CDM capabilities that we have not yet implemented.

So, I would ask you to look at those metrics again at three and six months. I think you will see some improvement, sir.

Mr. CLYDE. Well, I look forward to looking at those metrics and having the Department of Energy prove your statement because I just don't have the confidence right now in that, and I look forward to having a classified briefing.

Mr. Chairman, if you are willing to do that, I, certainly, will participate because, you know, for what the Department of Energy does this is not a good grade. Not at all.

So, if you would—if you would assist us in that, Mr. Chairman and Ranking Member Hice, if you would, I would, certainly, participate because this is a critical area of cybersecurity that I don't think is getting the attention that it should get at the Department of Energy.

So, and with that, I yield back.

Mr. CONNOLLY. Thank you, Mr. Clyde, and we will work with you to try to have a classified briefing, and the same grade on this subject leapt out at me as well. So, thank you.

The gentleman from Kansas, Mr. LaTurner, is recognized, and then the chair is going to hand over management of this hearing to the gentlelady from California, our vice chair, Ms. Katie Porter, to ring us out while I go vote. Thank you.

Mr. LATURNER. Thank you, Mr. Chairman.

Ms. Harris, I want to reask a question to see—that I didn't feel like there was a great answer to that my colleague, Ranking Member Hice, asked a little bit ago. What are some of the reasons that agencies may not meet the deadline with the rollout of the EIS program?

Ms. HARRIS. Well, some of the reasons are it is not an agency priority. They don't think about the transition until the deadline is on the horizon, unfortunately. So, it is really about proper planning and agencies—in looking at the previous two transitions, agencies have been poor planners in that regard.

But I also think Mr. Spires' comments about IT work force is also——

Mr. LATURNER. Well, what happens——

Ms. HARRIS [continuing]. very valid in this regard.

Mr. LATURNER. What happens when they fail—when they fail to transition? What is the consequence?

Ms. HARRIS. When they fail to—the consequence there, unfortunately, is one where GSA has to offer a bridge contract to extend the current set of contracts so agencies are able to—to be able to have more time to move over to the newer set of contracts.

And as a result of that, agencies are not taking advantage of the lower costs and rates and better services from the new contracts. So, when you take a look at the transition to networks, agencies lost out on $329 million in savings.

Mr. LATURNER. Talk to me about the national cyber director. How could the national cyber director be involved to strengthen Federal agency cybersecurity posture? It is relatively new, and I would just—I would like your take on that.

Ms. HARRIS. Well, we are very supportive of that position and the executive order that is put in place. We have ongoing work and also we will be starting new work to take a look at how agencies are implementing that executive order as well as taking a look at that position.

So, unfortunately, I don't have any more information other than that at this time for you.

Mr. LATURNER. OK.

Mr. Cavallo?

Mr. CAVALLO. If you talk about the—thank you for that question. Is it about the national cyber position?

Mr. LATURNER. Well, yes. I would love to hear your response to that quickly as well and then I have another question for you.

Mr. CAVALLO. Sure. Again, as we have heard from a number of experienced leaders on this panel, measuring cyber is very difficult, and I think we all can work together to improve that. So, I am looking forward to see what that additional guidance is.

In my previous role at SBA, I did two pilots on cyber with CISA and DHS and OMB on using newer technologies to improve cyber across an agency. So, I think—you know, I am looking forward to getting that type of leadership from that position.

Mr. LATURNER. Thank you for that.

Can you explain why your agencies failed to meet the deadline for transitioning to updated EIS contracts, and how will you pre-

vent work and operational interruptions down the line as we move closer to the 2023 expiration of the current contracts?

Mr. CAVALLO. Yes. So, and thank you for that question about the EIS contract. You know, I joined OPM, you know, about a year ago and that contract was already in competition.

We were very late in awarding it as an agency. In fact, the first scorecard came out where we had enough—we didn't have a contract in place to even transition to.

In the time since then we have awarded that contract in April. I am pleased to tell you that we are actively moving our network circuits and our telephone circuits now to that new contract and I fully expect that we will meet GSA's deadline.

So, sir, it was a late contract award. I needed to bring in additional resources. I have them on board, and we are actively moving now, and I am confident that we are going to meet the deadline.

Mr. LATURNER. I am glad to hear that and I am glad to hear you feel confident about it.

Mr. Chair, I yield back the rest of my time.

Ms. PORTER.

[Presiding.] Thank you very much, Mr. LaTurner. I will now recognize myself for five minutes of questioning.

Mr. CONNOLLY. Ms. Porter? Ms. Porter?

Ms. PORTER. Yes?

Mr. CONNOLLY. If I could just interrupt, because I am going to leave. But thank you.

I just want to say before I leave that I think this has been a very useful hearing. Clearly, we have consensus that we have got to, you know, make upgrades to the scorecard.

I think it is very important, though, to remember the scorecard is tied to law. We passed a law that agencies must be in compliance with. So, we don't want the scorecard to go too far afield from making sure that the law is being implemented and that we have got metrics that can reassure us of that.

I think it is also important to note that, you know, the scores we are looking at need to reflect reality, right. So, how did we perform, for example, during the pandemic in terms of customer satisfaction, ability to perform, and I think any reasonable person would say, well, by and large, pretty well but there were uneven, you know, patches.

You know, we struggled with passports. We struggled with small business loans, in some cases, because of the volume and the changes in programming. We struggled with, certainly, IT systems at the state level in unemployment insurance.

We struggled at IRS to get those family checks out and direct payments to the American people during a pandemic where we were trying to make sure the economy didn't go off a cliff.

So, looking at that uneven performance tells us, obviously, not all of us deserve an A, that there remain problems to be addressed and, hopefully, that in the next iteration of the scorecard we are accurately capturing performance so that we can make the necessary improvements.

Thank you all so much for participating today, and I now hand over the gavel to the most distinguished vice chair in the history of the U.S. Congress, Katie Porter from California.

Thank you, Ms. Porter, for yielding.

Ms. PORTER. Thank you, Chair Connolly.

In December 2021, President Biden issued Executive Order 14058, which directs Federal agencies to deliver services to the public more effectively, more efficiently, and consistently.

And those—these services that we are talking about include really important things to the American people like applying for a loan, giving small business counseling, requesting documents like a passport or a Social Security card.

Mr. Cavallo, your agency, the Office of Personnel Management, was one of the agencies specifically identified in the executive order, correct?

Mr. CAVALLO. Yes. Yes, ma'am.

Ms. PORTER. How is OPM implementing the requirements of the executive order?

Mr. CAVALLO. Great. Thank you for that question.

My predecessor, the current Federal CIO, had already started OPM on looking at the customer journey and, in fact, we got a head start on that.

One of the other keys is—so the first thing you want to do is look at what you are putting your citizens through to be able to work with your agency—how many times do they have to re-enter their name and address and things like that that we can all do better on.

The second part is having a digital services team. I have hired that team onboard to help lead that modernization effort. So, we are well on our path. We have a pretty extensive customer journey map now.

In my testimony, I highlighted that, you know, OPM touches the Federal employee from before they become an employee to their employment all the way to their retirement, and we are looking to streamline and improve that interaction.

Ms. PORTER. Great. This, actually, is a perfect segue to my next question.

In the executive order OPM was tasked, as you just said, with working with other departments, in part because Federal agencies and Federal employees touch other departments.

One of the things specifically mentioned was to creating a more streamlined process for borrowers seeking student loan relief through the Public Service Loan Forgiveness Program.

Can you share any information about how that process is going, what the streamlined application will look like?

Mr. CAVALLO. Thank you for that question, Congresswoman.

I am not all that familiar with where we are on that status so I would like to get back to you with the details on that.

Ms. PORTER. I would appreciate that, and, obviously, you are just—you know, the Department of Education and other agencies have a role to play here, too.

But since your testimony, I think, encouragingly suggests that OPM is doing—is a little bit ahead of the curve compared to other agencies with the executive order, I think it is really important that you bring that expertise to bear on this Public Service Loan Forgiveness Program.

You know, the Biden administration has taken action to expand the eligibility for that program, broadening the type of loans that qualify for forgiveness, automatically enrolling service members and public employees in the program.

So, thousands of people are on the path to loan forgiveness for the first time, meaning that they are closer to being able to save for retirement, cover the costs of childcare.

But the changes to the Public Service Loan Forgiveness Program are temporary. Borrowers have until October 31, 2022, to make the necessary changes to their loans that are required for eligibility.

So, Mr. Cavallo, I would love if you could followup with me on what you learn about when that streamlined application will be available for borrowers to use, because I don't want to hear that they are only going to have two weeks or a month because people need to get their mail and open their mail and read their email, and even in a streamlined process it takes time.

Is that something you could respond back to me on?

Mr. CAVALLO. Yes. Thank you. We will definitely followup with you on the status of that.

Ms. PORTER. Great, because we have nine months to go and I would like to give the American people some portion of that to do their part of this process. Thank you so much.

I will now turn to Ms. Harris. How can the FITARA scorecard accurately measure agency efforts to improve service delivery?

Ms. HARRIS. I think that is a very good question. I think that it is something that we need to work very closely with you and the subcommittee on as well as with OMB to really collaborate on the data that is available, publicly, because that is really the main driver for what we can use as a metric, to what extent data is available, whether it is public or not, or if it is—and if it is systematic or if it is something we have to manually collect. So, that is something that we will have to work with you on.

Ms. PORTER. OK. So, you identified two sort of variables there. One is public, and what is public is currently what can go into the FITARA scorecard—only public data—and the other is sort of how easy it is to collect this data on a regular basis.

I wanted to ask a little bit more about the public data because I think using that alone can make it really difficult to measure how well agencies are actually meeting their obligations.

Mr. Spires, in your written testimony, you said that nonpublic data in the scorecard would, quote, "provide a more accurate grade of an agency's cybersecurity posture."

Can you say a little more about the benefits of using at least some nonpublic data in future FITARA scorecards?

Mr. SPIRES. Yes. Well, thank you. Yes. As was kind of evidenced by some of the discussion we just had about going into a classified setting, there is a lot of sensitive data in and around cybersecurity and an agency's posture and, obviously, we don't want to—we don't want to have public data that is going to actually endanger an agency in any way.

And I think in order to get an effective and a comprehensive score around cybersecurity, we should change that. You know, I know we want to use public data, but we—I think that is the one area we should, really, probably open this up and say probably ef-

fective to use some nonpublic data in arriving at a particular score for cybersecurity.

Ms. PORTER. Yes, and I think we all agree that this is sensitive information. Congress also receives sensitive information all of the time and we have a lot of protocols in place to do that, and I think it is important that we think about making sure that Congress has the tools to do effective oversight.

Would you say that when you were chief information officer at DHS that the results of the FITARA scorecard were sometimes at odds with where the agency actually was, based on the internal data or the confidential data that you had?

Mr. SPIRES. Well, I actually served—I was involved in testifying about FITARA being passed. So, I actually had left the agency prior to the scorecard existing.

But as someone that has been on the outside looking in and still very involved in these issues, yes, I think that—I think many CIOs feel like they are doing better in some areas, maybe even worse in some areas, than what the scorecard was reflecting.

You know, as we say, it is difficult and I know GAO has a difficult challenge here trying to come up with—and you do, too—come up with effective measures that are based on just available data.

I would say that some of the—not just my testimony but some others are saying, hey, let us go after and create some new data when we need to or gather it in a way that can be more effective in enhancing the scorecard.

Ms. PORTER. That actually goes to my last—not quite my last question but I am getting there.

Ms. Kent, in your time as a Federal CIO, which IT-related metrics remained the most relevant over time, and then if you could also identify where do you think—and I am going to ask Mr. Powner to respond to this, too, after you—where are there new or updated—opportunities for new or updated metrics?

I mean, we want to keep things narrow enough that we are motivating the agency to make progress, but we also have to make them broad enough to stay relevant as technology evolves.

So, can you just give the committee some information to—about which ones stay really useful over time and where might we need to have a more regular updating process?

Ms. KENT. I think some of the categories—so, you know, we used data center kind of as a proxy for modernization. But that specific metric, you know, has now kind of met end of life, and you heard a lot of people talk about modernization, are there other—it is still a theme, it will be an ongoing theme—are there other things.

The same in cybersecurity. We are using some of the FISMA components as a proxy, but we have talked about, you know, timeliness. So, zero-trust, implementation progress, encryption status, endpoint detection, information sharing—those may be things that are more timely, and I think as we look at metrics, you just touched on the importance of the customer experience.

For agencies to actually understand their progress and for Congress to understand their progress, there is some information that we don't currently collect and maybe some of it, you know, therefore, is not public or doesn't meet the current paradigm.

GSA did a survey about citizen perceptions of government websites. There is other places where that information has been done and already published publicly.

So, maybe there are ways that we can bring those metrics into the scorecard and be creative in the data that we use to do that so that not only is it more timely, it is reflective of an outside looking in, which is how, particularly, in the customer experience area citizens are judging us.

Ms. PORTER. That is really helpful, especially as we think about making sure this is—that this executive order, which doesn't always happen despite best efforts and hard work by people, doesn't always—executive orders don't always translate into executive action and there is a pathway to getting there.

And, I think, one of my passions in Congress—and I think we have all know how passionate my chair is about FITARA—but one of my real passions in Congress is trying to design laws up front with the right amount of oversight built into them.

And, obviously, FITARA is an oversight law, but I think this executive order is a good example of thinking ahead at the time you issue the executive order of telling agencies how you might be evaluated for the progress you are making on customer experience, not just to say make a better customer experience and then mileage will really vary.

Mr. Powner, did you have anything that you wanted to add about sort of balancing competing priorities between existing metrics, new metrics, public data and nonpublic data, as we think about updating the FITARA scorecard?

Mr. POWNER. Yes. So, a couple things, Representative Porter.

I think it is very important, your question about service delivery and the customer experience. So, it is a major priority with the executive order and the whole bit.

The legacy challenges we face on, like, benefits that citizens expect, it is going to be difficult to really knock it out of the park on customer experience with some of our back-end legacy systems.

So, that is where, I think, the scorecard really needs to evolve to improve the customer experience, address the legacy challenges, but it also addresses, as Representative Lynch mentioned, some of the security vulnerabilities associated with legacy systems.

So, clearly, what we heard in today's hearing is we need to focus on legacy modernization for a number of reasons. The other thing that came out of this hearing, I think, is there is plenty of opportunity to focus on new cyber metrics.

I think the administration's focus on the executive order and zero-trust—if you look at the tenets of zero-trust like multi-factor authentication, how we encrypt our key traffic, there is a way to measure that stuff and to really progress our cyber posture.

And then, finally, we have a gap in terms of a skilled work force when it comes to IT and cyber folks. We need to find a way to highlight on the scorecard where we are at with our work force, what the gap is, and how do we fill that gap. So, those are a couple of the key things.

But I would say legacy modernization, cyber, and work force are three things that, clearly, came up on areas of focus down the road and I think the panel here, there were a lot of great suggestions on metrics and data that we can pursue, and I just commend this committee for looking at how we evolve the scorecard because this is the right way to go.

Ms. PORTER. Excellent. And because I really am an equal opportunity questioner today, Ms. Dunkin, I just wanted to turn to you in closing and ask is there anything that you would like to add? Any comments on that modernization—I am sorry, the work force recruitment issues and how you feel?

I mean, Department of Energy is one of the more sort of science-oriented agencies. If you guys are having trouble, I would say it is likely that everybody is having trouble.

Any suggestions on how we might measure that work force pipeline and how agencies are doing it at finding and identifying those staff members?

Ms. DUNKIN. Representative Porter, thank you for that question. I think we might have to take some thought about how we could measure the pipeline for recruitment.

I think, you know, it is a hard—it is something—it is very hard to measure the talent pipeline. It is easier to measure sort of the things we are doing to improve the talent pipeline—for example, ensuring that we are looking in the right places to get a diverse talent pool, ensuring that we are providing good pathways into our organizations through internships, through direct hire, and also dealing with the issues where pay is just not in a place to attract folks.

I mean, DOE—in our labs, we have the ability to work on different pay structures. But that doesn't help me with my Federal staff, right. So, our labs can do one thing. I have many more constraints in terms of our ability to pay those folks at the market and so we are looking at those flexibilities as well.

So, I think it may be easier to get meaningful measurement out of the activities we are taking on to improve the pipeline than measuring the pipeline. We do need to look and make sure we have got a diverse and deep pipeline. But I think the first piece about what are we doing is the most important thing we can do, I think. Thank you.

Ms. PORTER. Excellent. I think we are ready to wrap up.

Ranking Member Hice, or is there another Republican sitting in, if you want to make a closing statement I am happy to recognize you.

[No response.]

Ms. PORTER. We all had to go vote. So, that is what happened to everybody. We apologize. I just—I am in my kitchen so I was able to vote remotely and, therefore, be able to continue this hearing.

OK. I am going to go ahead and wrap up and close. I want to thank each one of you for your remarks, for your flexibility, too, in coming together in one panel so that we could have as much time with you as possible and thank my colleagues for participating in this important conversation.

With that—without objection, all members will have five legislative days within which to submit extraneous materials and to submit additional written questions for the witnesses to the chair, which will be forwarded to the witnesses for their responses. I ask that witnesses please respond as promptly as you are able.

With that, the hearing is adjourned.

[Whereupon, at 10:53 a.m., the subcommittee was adjourned.]