PROJECT FEDERAL INFORMATION TECHNOLOGY: MAKE IT WORK

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 16, 2022

Serial No. 117–103

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

48–613 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
MIKE FLOOD, Nebraska

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, Massachusetts
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

INDEX OF DOCUMENTS

PROJECT FEDERAL INFORMATION TECHNOLOGY: MAKE IT WORK

Friday, September 16, 2022

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

The subcommittee met, pursuant to notice, at 9:07 a.m., in room 2154, Rayburn House Office Building, and via Zoom; Hon. Gerald E. Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Lynch, Khanna, and Hice.

Mr. CONNOLLY. The hearing will come to order.

This June, the Office of the Federal Chief Information Officer, led by today's witness, Clare Martorana, published the Information Technology Operating Plan. This plan outlined the Office of Management and Budget's strategy to maximize the impact of Federal IT funds.

As someone who's dedicated decades to championing IT modernization across both the private and public sectors, I was heartened to see the plan encompass many of the long-range priorities of this subcommittee.

During our tenure, we've held 14 hearings, released 14 scorecards, grading agencies' implementation of the Federal Information Technology Acquisition Reform Act.

FITARA promotes proper IT practices across Federal agencies. Every scorecard iteration reflects contemporary shifts within the IT landscape, evolving as needed with changes in modernization and cybersecurity best practices to hold agencies' CIOs accountable for ensuring proper IT postures.

Since the scorecard's inception, agencies have saved an estimated, according to GAO, $29 billion. There aren't many bills that can claim that.

Similarly, the Federal Chief Information Officer's new technology plan provides a solid roadmap to continue the vital work of improving our Federal IT systems to better serve our constituents.

Today, we will hear the Federal CIO present her vision for the future of Federal IT.

This moment is a crossroads in how government operates. The pandemic fundamentally changed what people expect from their government and how they access programs, information, resources from it. We do not want to lose any lessons learned, and we want to empower Federal CIOs to scale IT solutions that, in fact, work.

Today we will explore in-depth the Federal CIO's four IT focus areas: cybersecurity, IT modernization, digital-first customer experience, and the use of data as a strategic asset.

I'm pleased that cybersecurity remains a top priority for the Biden administration. In 2020, the SolarWinds' supply chain cyberattack blindsided top security experts across the world. This attack catalyzed the reevaluation and n modernization of our Nation's cybersecurity strategy.

Since that attack, OMB has reengineered a new risk-based cybersecurity regime using new metrics to measure and assess Federal agencies' cyber posture. In December 2021, OMB shifted government toward a zero-trust architecture, focused on ground truth testing, observable security outcomes, and automation.

Today we'll hear a lot more about the work OMB has done to change the culture of Federal IT, and we're eager to dig into their recently released memorandum on enhancing the security of the software supply chain through secure software development practices.

We'll also discuss how the subcommittee can work with OMB to ensure that we have publicly available data for the FITARA scorecard, holding CIOs accountable, and empowering them to implement cybersecurity lessons.

Additionally, as co-chair of the IT Modernization Caucus, I am quite familiar with the problems caused by agencies' failure to modernize. A GAO report found that, quote, "The consequences of not updating legacy systems have contributed to, among other things, security risks, unmet mission needs, staffing issues, and increased costs," unquote.

Successful modernization demands constant action and nimble solutions that keep pace with rapidly shifting IT ecosystems. I'm proud to have helped successfully secure, for example, a revolutionary $1 billion for the Technology Modernization Fund. The TMF reimagined the way agencies could receive financing, offering opportunities outside of the traditional appropriations process, facilitating long-term planning, and providing expert assistance. To date, the fund has awarded, I believe, almost $600 million to 28 unclassified projects across 17 Federal agencies.

Despite the massive investment, agencies need more. At our May hearing with TMF's executive director, she noted that 60 agencies have applied for over 130 projects, totaling $2.5 billion in prospective funding, more than double what was provided by Congress. We must continue to support this fund and seed agency efforts to ensure that their IT systems are prepared.

I also want to highlight the Biden administration's executive order focused on improving Federal service delivering customer experience. These combined factors are key to rebuilding the public's trust in the government and preserving our democracy.

The Federal CIO has told this committee in previous hearings that improving customer experience is their passion. We aim to find ways to jointly hold agencies accountable for making it easier for all people to interact with their Federal Government through user-friendly websites and careful attention to accessibility.

Every day, people transition seamlessly between the digital and physical worlds. The pandemic pushed more of us to telework from

home, scan a QR code, or order dinner at a restaurant, or zoom with loved ones, or even with your colleagues here in Congress, also loved ones.

In the same way we depend on technology to serve the public, serving the public well depends on data. Data ensures that only those who qualify for Federal benefits can access them. Data helps agencies create hiring strategies to get the talent they need to serve the American public. Data helps agencies prioritize IT investments and finds ways to share services across Federal agencies.

Today we're interested to hear from Ms. Martorana on how government can maximize both cost savings and better service delivery. I will also seek to find opportunities for the subcommittee to continue to work with the Biden administration to ensure that our government is meeting this pivotal technology moment.

With that, the chair recognizes the ranking member, Mr. Hice of Georgia, for his opening statement.

Mr. Hice.

Mr. HICE. Thank you very much, Mr. Connolly, Chairman. I appreciate you calling this hearing. I must say you look good there in the hearing room. I wish I was able to join you in person, but I've got a full day here in the district after this hearing. But I do thank you for calling this—this hearing today.

As I've said to you before, I really appreciate your insistence on bringing Biden administration witnesses before us. So, I appreciate that as well.

And, Ms. Martorana, I appreciate you being here today, and sincerely express to you my condolences for the loss in your family, for not being able to join us in July. I hope you and the rest of your family are doing well as you deal with the grief of a loss like that.

But as we gather here today, none of us can understate the importance of Federal information technology. We all know that it's critical, and I cannot think of any aspect of our government that does not rely on information technology to deliver services and the jobs that they are called to do.

There's an underlying assumption that the vast amounts of funding somewhere in the neighborhood of $100 billion a year will somehow deliver the intended results. But in my time in Congress at least, and certainly during my time as ranking member of this subcommittee, I've learned that it's probably not wise to make that assumption.

Our hearings just, for example, with the IRS have shown that simply spending billions and billions of dollars and then waiting decades does not mean that agencies will get their IT house in order.

And while my Democratic colleagues claim the source of the problem is lack of funding, I, quite frankly, reject that premise. Simply pouring more money into a black hole is not a solution. What we need is solid oversight that is backed by reliable information in order to determine the true state of our Federal IT, to determine whether Federal IT projects are delivered on time and on budget. All of that requires oversight. It requires accountability. Whether IT projects deliver the intended results and whether Federal systems and networks are secure. I am far from convinced that all of this is taking place.

In today's hearing, I'm eager to learn more about what exactly we do know about Federal IT and what ability the Federal CIO has to drive behavior and improvement. That's a question that we should know but, frankly, I don't know. So, I want to have that answer today.

I also want to voice my concerns about what seems to be a pattern from this administration to ignore the law and the clear intent of Congress. The law requires OMB to develop management goals, the cross-agency priorities, or the CAP goals.

Congress wanted a long-term management blueprint from each administration for improvement and reform. These not only should help improve agency performance, but give us here who are, in essence, the de facto board of directors of the Federal Government, a map for effective oversight. Yet the Biden administration has ignored this requirement.

The CAP goals were due in February of this year, but it didn't happen. And at least I'm not aware of any discussion of this matter between the administration and this committee. I'm not aware of any request for an extension. They just simply did not do what the law requires. And, frankly, this directly impacted the last FITARA scorecard on perhaps the single most important issue and category, and that is cybersecurity.

So, look, the administration simply cannot comply with the law when they want to and ignore it when they want to. There must be accountability.

And with respect to the Technology Modernization Fund, this administration is ignoring the intent of the underlying Modernization Government Act. The focus of the TMF and the broader MGT, as we'll call it, was to modernize government IT systems. That meant doing away with the types of ancient systems that still run and—too many of our vital government programs. In addition, the tenet of the TMF was that it would create an efficient cycle.

So, to paraphrase none other than Democratic Leader Steny Hoyer, agencies were to reimburse the fund ideally through these savings that were gained from doing away with costly legacy systems. But the Biden administration has opted for partial or even minimal reimbursements. I want to know why.

It's also emphasizing cybersecurity and customer experience projects, which in and of themselves are fine, but doing so rather than retiring old systems.

Taken together, even if the law requires these practices, again, it's not that these practices in and of themselves are bad, but it simply and clearly is not the intent of Congress. So, why is the administration doing this? We need answers.

Does the savings-based model of the TMF not work or is it simply inconvenient? This committee needs to know.

And what progress is being made to retire legacy systems? Is there even a definition of what a legacy system is?

Do we know how well the billions of IT funding are being used?

Is the Federal IT dashboard, which is supposed to give us the answer, is it at all reliable?

Where does the underlying data come from? Is it even accurate data?

Are requirements and definitions uniform? If not, what would it take for this to be the case?

Finally, what ability does the Federal CIO have to drive and produce better practices?

The title sounds lofty, indeed, but the GAO notes in a new report that the Federal CIO position was never even established in statute. The first reference of a Federal CIO came in a press release, the actual role of the administrator of the Office of E-Government.

So, regardless of the title of the Federal CIO, certainly it would suggest the ability to direct agency CIOs and take a leading role. So, I want to know: Is that the case? Do you have that kind of authority?

If Congress attempts to hold the agency CIOs accountable, as we do through the FITARA scorecard, then should we not also hold the Federal CIO accountable? But if we do, for what are we holding that position accountable? We don't even have a job description.

So, I'm eager to have these questions answered today and in future conversations.

Again, Chairman Connolly, I want to thank you for holding this hearing. And, with that, I yield back.

Mr. CONNOLLY. Thank you, Mr. Hice.

And you've raised some really good questions. And I saw our witness shaking her head "yes" to some of what you were saying, so I look forward to getting some answers to those as well, and that's why we're having the hearing today. And I thank Ms. Martorana for joining us.

So, we do have one witness, Clare Martorana, who currently serves as the Chief Information Officer of the Federal Government.

I would ask—Ms. Martorana, it is our habit, our practice, to swear in all witnesses before this committee—if you would rise and raise your right hand.

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

Ms. MARTORANA. I do.

Mr. CONNOLLY. Let the record show the witness answered in the affirmative. And I thank you so much.

With that, you are invited to provide us with a five-minute summary of your testimony. And, of course, your full statement will be entered into the record.

Welcome.

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

Ms. MARTORANA. Chairman Connolly, Ranking Member Hice, and members of the subcommittee, thank you so much for the invitation to testify about the state of Federal IT and to update you on our progress to highlight where we're heading.

The President believes the government needs to deliver for all Americans, your constituents, and I do too. It's technology that powers our ability to deliver on this promise.

Through the work of this subcommittee, you've provided consistent bipartisan support of IT modernization, reducing wasteful spending, and improving project outcomes. You've advocated for

Federal CIOs to have a seat at the table. Now we need to give them a voice upstream in the decision-making process to ensure agencies are making the right IT investments at the right time, to ensure—to have a simple, seamless, and secure customer experience.

Over the past two years, customer expectations have risen to new levels, as the chairman mentioned in his opening statement. We must keep pace and accelerate even faster. We can deliver as a government on par with our favorite consumer brands. By delivering products and services incrementally, with the right technologists and senior level support, it's not only possible, it's happening today in the Federal Government.

Veterans can schedule appointments, refill a prescription, get push notifications for their claims and appeals with VA's new mobile app. And that new mobile app has a 4.8 out of 5-star rating, which is incredible.

Recently married residents in five states, including my now home state of Georgia, who want to update their Social Security card to reflect their new name can now take care of that online versus traveling to a Social Security office and filling out paperwork.

And passengers are now able to use an authenticated mobile ID during TSA's airport screening pilot, decreasing the processing time, and enabling a touchless experience.

Through this work, we are demonstrating to agencies and the Federal work force that change is possible. We are building trust with the American people when they interact with our government. And, importantly, we are inspiring others to join us serving this great country.

As Federal CIO, I have a really unique vantage point and the honor of bringing together leaders across government to drive progress. We are collaborating closely on cybersecurity, which remains our top priority. Working with the Office of the National Cyber Director and our OMB budget colleagues, we are assessing where agencies are on their IT journey and ensuring they are making the right investments to strengthen their cybersecurity foundation and accelerate IT modernization. This work will place agencies on a sustainable path to maximize investments from Fiscal Year to Fiscal Year and from administration to administration.

Second, we are maximizing the impact of the funds entrusted to us as center-of-government technologists by aligning our work around strategic IT priorities, as you mentioned, Mr. Chairman. Outlined in our Federal Information Technology Operating Plan, the Office of the Federal CIO, the United States Digital Service, and our colleagues at GSA are aligning resources and tech teams to administration priorities and driving innovation through funding models like the Technology Modernization Fund.

And third, we are providing technologists with the executive support needed to have a voice in agency C-suites. The government experience will improve by having technologists early and often in agency planning. Technologists are key to vetting strategies to drive down the failure rate of IT investments and reduce administrative burden for the Federal work force so they can work smarter, not harder.

With each new product and service we launch, we're closing a chapter on the paper process, sadly, the main way that we are still conducting much of our business across government. Paper is not only slow and antiquated, it's inaccessible to the digital world, it's a burden for the Federal work force to have to process, and it does not meet the bar for modern service delivery. We must and can do better.

Working together, we have the ability to drive digital transformation across the Federal enterprise. Partnering with agencies, our industry partners in Congress, we can deliver to the American people the government they deserve.

So, thank you so much for the opportunity to testify today, and I look forward to your questions.

Mr. CONNOLLY. Thank you so much, Ms. Martorana, and we're glad to have you.

And we will now turn to questions. And the chair recognizes the distinguished Congresswoman from the District of Columbia, Congresswoman Eleanor Holmes Norton, for her five minutes of questioning.

Ms. Norton.

Ms. NORTON. I thank my good friend, Chairman Connolly, and I appreciate this important hearing.

We all know that the Federal CIO is responsible for overseeing government IT security, and that includes everything, budget and planning, and all the rest of it.

During the pandemic, we saw a further acceleration of government's reliance on Federal information technology to get individuals and families and businesses, to get them what they needed from government. These changes made it paramount that the Federal CIO sets enterprise-wide policies and structures that help agencies get IT right.

Ms. Martorana, with so many responsibilities, how do you determine your priorities? And what are your current priorities as the Federal CIO?

Ms. MARTORANA. Thank you so much for that question. You know, I fulfill many statutory responsibilities on behalf of the Director of OMB. The role is overall oversight of information security, management of IT resources, implementation of eGovernment services. And I also serve a role to convene across IT—across the entire IT enterprise of the Federal Government.

So, we determine priorities based on both the environment that we're operating in when the administration began. We were in the midst, to your earlier comment, Mr. Chairman, on SolarWinds and the devastating impact that that had, not only to the nine impacted agencies but to every single Federal agency. Because when we do have a cyber event, we do have to both investigate and potentially remediate across our entire enterprise, because if one of us is impacted, all of us are potentially impacted.

So, the role of the Federal CIO is really helping Federal CIOs in agencies manage this very complex operating environment with a complex set of rules, regulations, binding operational directives. And it is really incumbent upon this role to make sure we are playing an oversight role, that we are measuring where we are able to, that we are sharing best practices across agencies.

Every Federal agency and CIO that I work with, we're all trying to solve the same problems. We don't want to start from a blank piece of paper. So, when one agency goes on an IT modernization journey, for example, we want to make sure that we share those best practices across the entire Federal enterprise.

Ms. NORTON. Well, may I ask you: How do you plan to operationalize CIO's leadership and accountability across Federal agencies?

Ms. MARTORANA. Yes. Currently, Federal CIOs are responsible for making sure that their environment is safe, secure, and that they are fulfilling FITARA, FISMA, and the President's management agenda. So, we are receiving an enormous amount of data from Federal CIOs, which is really an important part of our entire—both our oversight mission at OMB as well as Congress' oversight mission.

Ms. NORTON. Well, as you know, empowering CIOs and then holding them accountable for using their authorities effectively is the goal of our subcommittee, its biannual FITARA scorecard.

So, may I ask you: How will you work with Congress to provide the public data and information that will help you in your efforts to highlight IT leadership and accountability?

Ms. MARTORANA. Yes. We work very closely. We try to be transparent in the reporting, so we have an IT dashboard which is publicly available. We also publish out in each agency's strategic plan. IT is a critical component of all of those. So, we are able to get a view, not only across the Federal Government from the compliance and reporting perspective, but also from the operational perspective.

Ms. NORTON. Thank you very much. My time has expired.

Mr. CONNOLLY. Thank you so much, Ms. Norton.

The ranking member, Mr. Hice, is recognized for his five minutes of questioning.

Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman.

Ms. Martorana, as you know, and I mentioned just a little while ago, OMB is required to issue the cross-agency priority goals with an administration's first budget submission. That would have been February of this year, and for some reason, the Biden administration did not submit the CAP goals on time. And at least to my understanding, I'm not aware of whether it's issued the CAP goals even now. And as I referenced just a few moments ago, during the FITARA scorecard hearing in July, the lack of the CAP goals prevented this subcommittee from receiving an accurate assessment of agency cybersecurity readiness.

So, my first question to you is really simple and that is: Why is the administration not complying with the law? Why are they not issuing the CAP goals on time?

Ms. MARTORANA. Thank you for the question. I do—I did hear a little bit about what happened after the FITARA hearing, and we take our role being responsive to Congress and the American people incredibly seriously.

It is my understanding that OMB is technically in compliance with GPRA. We are required to designate CAP goals, which we did on August 9 of this year. They are publicly available on *perform-*

ance.gov. We are required to do that by the end of the full first fiscal year, and that is this year. So, we are technically in compliance.

But your point is really valid. We need data to make sure that we have transparency, that our data is accurate, that it is available and, again, transparent, and actionable. So, I am in agreement with you that this is a responsibility that we have, and we are working hard to fulfill that responsibility.

Mr. HICE. Well, I would challenge a little bit that——

Ms. MARTORANA. Sure.

Mr. HICE [continuing]. that they're in compliance. The—they're clearly not in compliance. The CAP goals are due in February—that is not complicated—and they were not there. We could not perform our job in this subcommittee of Oversight in July with the FITARA scorecard because this administration is not in compliance.

We take it seriously. I know you said you do, and I don't have any reason to question you, but we in this committee take our job seriously, and we expect to have the information we need in order to do our job.

The Biden administration is ignoring the intent of Congress with respect to the Technology and Modernization Fund. The primary focus of TMF, as well as the underlying Modernization Government Technology Act, the primary focus was to make meaningful progress in retiring legacy systems. I mean, that's what we're trying to do. I personally have been in government agencies that are still using DOS programs.

Ms. MARTORANA. Yes.

Mr. HICE. For crying out loud, this is unacceptable. We have got to retire these old legacy IT systems. And this—the whole thing was to create savings which would then be used to reimburse the Fund.

But the Biden administration is only requiring partial or even minimal reimbursement in emphasizing cyber projects and customer experience projects. Again, in and of itself, nothing wrong with that, but it's not the intent of Congress.

So, you know, the question obviously is: Why should we believe that under your leadership the TMF has become nothing more than a slush fund?

Ms. MARTORANA. I really look forward to having a very robust conversation with you about this. The TMF board has always required repayment. We are focused on investing in projects that we know have a high likelihood of success. So, what we do is we actually have redesigned the entire TMF process.

When I joined, we had three staff on the GSA side that were mostly doing financial administration of the TMF. We have, in the last year, put technologists on the TMF PMO so that we work closely with agencies in the beginning of their initial project proposals. We review them, and we review them with a set of complex guidelines.

Are they—do they have the staff on the ground to do the work? Do they have the right procurement vehicles in place to do the work? Do they have the right contracting partners in place to do the work? What exactly—how are they designing the project that they are undertaking?

We have seen many IT failures across government mostly because we have not taken the time up front to build an incremental plan to do IT modernization.

So, I would look forward to working with you and your staff and doing a detailed review of any and all of the projects that we are supporting under TMF. I think within the next year you are going to see such dramatically improved outcomes from the TMF projects, because we are managing them in a completely different way than we did previously, by having technologists up front in every single part of the investment.

We review our investments quarterly. If people are not hitting their milestones, we do not give them additional funding. We have brought all of government together. If teams are failing at a component, we rally people together to be able to support them with the subject matter expertise that will help them be effective and efficient.

So, I look forward to speaking with you and your staff at any time about the way that we are changing fundamentally the delivery and the outcomes for TMF. But we are staying core to IT modernization and government, and repayment is a very critical part of that for the Fund.

Mr. HICE. Mr. Chairman, thank you. I hope we'll have an opportunity for further questions since there's so few members that are here.

But, Ms. Martorana, I appreciate your answer. But, quite frankly, I'm not convinced at all that you answered my question. But I hope we'll have an opportunity to speak further.

Mr. CONNOLLY. Let me assure the ranking member we will. We will. So, we'll have another round.

And if the—if I may followup just real briefly for clarification on one of the questions the ranking member asked. You—the Office of Management and Budget has allowed sort of partial repayment from TMF. Is that correct?

Ms. MARTORANA. Yes, that's correct.

Mr. CONNOLLY. And the legal validation of that authority was, in fact, either provided by or guidance was provided by approving that practice by GSA. Is that correct?

Ms. MARTORANA. By both GSA and GAO——

Mr. CONNOLLY. And GAO.

Ms. MARTORANA [continuing]. reviewed our repayment.

Mr. CONNOLLY. But if I understood your answer to Mr. Hice, but the intent, despite partial repayment, is full repayment.

Ms. MARTORANA. Absolutely.

Mr. CONNOLLY. Yes. OK. Just wanted to clarify that for the record. So, the fact that there have been partial repayments is not a substitute for the ultimate full repayment, but it's providing more flexibility.

Ms. MARTORANA. Correct. And we also, the appropriation—the American Rescue Plan appropriation was an emergency appropriation. We were dealing with dire circumstances in several agencies related to cybersecurity, and they did not have the ability to reprogram money quickly enough in order to meet the need at the agencies.

Mr. CONNOLLY. OK.

Ms. MARTORANA. So, TMF plays a really critical role in that way as well.

Mr. CONNOLLY. OK. I know we'll come back to that, but I just wanted to clarify that part of it. Thank you.

The distinguished gentleman from Massachusetts, Mr. Lynch, is recognized for his five minutes of questioning.

Mr. Lynch.

Mr. LYNCH. Good morning, Mr. Chairman, Ranking Member. Thanks for doing this hearing.

We've been here before, and I do share some of the frustration with the lack of progress.

Ms. Martorana, thank you very much for your efforts. Thank you for your service.

The last time we were together on FITARA, I had asked about the Log4j vulnerability. As you may remember, CISA reported that that vulnerability, which affected millions and millions of servers, was one of the worst vulnerabilities discovered in many, many years.

Now, during our last hearing on this, we still didn't have a lot of information, and I did not get a satisfactory answer. But it'll be a year in December that we—we warned people about—the government warned this—people about this vulnerability. And I'm wondering what the level of progress has been in terms of trying to fix all of the—all of the vulnerabilities that have been discovered because of this Log4j code vulnerability.

Do you have any type of assessment or report on that? I understand that the fix is rather cumbersome and complicated, so it's not like you just do a patch. It's a very complicated process. And because Apache Log4j is so—it's open source, so all these—all these software developers sort of imported it and now have, you know, lent themselves to that vulnerability.

I do also want to, before you answer, I'm also disappointed that it was Alibaba that discovered the vulnerability and not our folks. Doesn't give me much confidence. But, you know, after the fact, I think Mandiant and CrowdStrike suspected that it was actually Chinese hackers that were able to implement this vulnerability across so many of our systems, including the government.

So, where are we in cleaning up this mess?

Ms. MARTORANA. Yes, thank you so much for that question. You know, cyber threats facing Federal agencies and the software that underpins the work of our Nation has to be developed in a resilient and secure manner. So this week, we released OMB memorandum, enhancing the security of the software supply chain through software—secure software development practices. And that is a critical part of how we are going to direct agencies to make sure that we're only using software from producers that comply with secure software development practices and standards.

So, Log4j is quite complex. I think Director Easterly said it was one of the most challenging software vulnerabilities that she had seen in her career. And Federal agencies still continue, as does the private sector, to try and deal specifically with Log4j and the associated challenges in actually determining where it is, how it's being executed, and how it can be remediated.

Mr. LYNCH. Yes. Well, I understand. You know, we've got some lessons learned, right? So, we're not going to do that again. I appreciate that. But it's an outstanding vulnerability that's still extant, and I'm just worried about the situation with that process. It's—you know, the problem is locating the vulnerability and then implementing the fix. So, that's taking a long time. And I'm not hearing any timetable or percentages in terms of where do you think we are in, as I said, cleaning up that mess.

So this is, again, a year later. So, I'm still asking the same question, and I'm not really getting an answer that's helpful. I do——

Mr. CONNOLLY. Mr. Lynch, if I may interrupt. I'm going to—if you wish, I'm going to extend your questioning for another five minutes.

And then, Mr. Hice, we'll come back to you also for another five minutes. OK?

Mr. LYNCH. Thank you. Thank you. Thanks, Mr. Chairman. I really do appreciate it. Thank you.

Ms. MARTORANA. And——

Mr. LYNCH. So—go ahead. I'm sorry.

Ms. MARTORANA. And, Mr. Lynch, I would—I will direct—take your question and direct it, working with my colleagues at CISA, and get back to you with some more specificity around timelines and percentage of remediation that's being completed, if our colleagues at CISA have that data.

Mr. LYNCH. Thank you.

And what I might suggest is, let's just take the government vulnerability, because this is so widespread, so many companies imported that software, that maybe—maybe we can just get the—our arms around the damage to government servers and clean that part of it up. And then, as you say, we've cleaned up our supply chain and acquisition process. Maybe we can firewall this thing. But maybe we can do that.

And the best use of our time might be to do a classified, and you can tell me then or CISA can tell me what the vulnerabilities are right now, in a secure setting, and at least make me a little more comfortable that we're actually making progress, if those answers can't be given publicly.

The second piece I had is I know that—I know that President Biden chose to discontinue some of the—some of the practices, cyber practices that were implemented by the previous President. And I'm wondering if that transition, where are we with that? And what's the nature of our changes in terms of, you know, gathering data and that practice?

Ms. MARTORANA. Yes, I was fortunate to serve in the last two administrations. And we have not stopped focusing on cybersecurity. I have not seen anyone take their foot off the gas. This is a team sport. And while we might have to look at different ways to collect data, the burden that we put on agencies by constantly asking for manual data calls is really burdensome and we don't always get clean data. We don't certainly get machine-readable data which would allow us to automate some of our reporting.

So, I think we have a real opportunity to continue to invest in getting more real-time reporting based on better tools that would be available both from at the agency level and also at the OMB

level, so that we are not manually compiling these data-sets trying to, you know, clean the data, make sure that it is accurate and also then actionable so we can make really informed decisions from it.

So, I look forward to continuing the work on that, and I think that that is something that will carry through. It carried through previous administrations, and it will carry forward into the next administration.

Mr. LYNCH. All right. Can you at least tell me—so the metrics have changed in terms of, you know, data gathering from the Trump administration to the Biden administration. I'm not sure, you know, where we are in that transition and how successful that's been so far. But what's the nature of the transition? Is it tightening or refocusing? Can you help me a little bit with that?

Ms. MARTORANA. Yes. We are consistently looking at the data that agencies are providing us and trying to figure out the best way that we can assess risk from that agency data-set. And so we will constantly refine the data as we both deal with different threats, as well as make informed—different and informed decisions and also make progress.

So, I think that we will never have a single set of data that will accurately reflect the threat environment that we're dealing in, but we will continually refine that. But it is really critical that we are—continue to be transparent and responsive to Congress. So, I think that is our foundational operating model.

And I do understand there was frustration with this CAP goal issue, but I can really assure you that the data that we are collecting will be more accurate, it will be more actionable, and it will help us work together to make sure that we're making the right investments to help these agencies remediate many of these really critical security issues.

Mr. LYNCH. OK. Well, thank you for your efforts. And we'll continue to talk and—but I do appreciate your efforts.

And, Mr. Chairman, thank you so much for your courtesy. Thank you to the ranking member as well. Thank you. I yield back.

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

The ranking member is recognized for a second round of questioning.

Mr. Hice.

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

Ms. Martorana, can you give me a definition of a legacy system?

Ms. MARTORANA. I'll give you my definition of a legacy system. A legacy system is a system that does not meet the mission needs of an agency.

There are circumstances where an older system, if it is able to be patched, if it is available, high availability, sometimes we are able to run on some legacy systems that actually have still—have operational viability. But where—where I consider a legacy system that wholesale needs IT modernization is a system that is failing an agency's mission so that we cannot deliver the right services to the American public.

Mr. HICE. Does anyone else share your definition?

Ms. MARTORANA. I think a lot of my IT colleagues share that same definition.

Mr. HICE. We need—you know, look, and it's a good definition. I don't have any problem with your definition. But we don't have an official definition. Somehow you have your definition, somebody else has theirs. And, you know, the next question obviously is: How good are we doing at retiring legacy systems? We're spending hundreds of billions of dollars and we're not—we seem to get nowhere in retiring these old systems.

A scale of 1 to 10, 10 being perfect, how well are we doing on retiring legacy systems?

Ms. MARTORANA. I—that's a tough question to answer. I would probably give us a 5 out of 10. I think that it is——

Mr. HICE. I think you're being very gracious, but I'll accept that.

So can—where can we get a pretty accurate appraisal of the billions of dollars in IT funding, how it's being used?

Ms. MARTORANA. I think the IT Dashboard is the first foundational place to look at what those investments are. Also, each agency budget has very—has specificity online items related to IT projects. Also, programs within those agencies, there's also specificity on IT investments.

Mr. HICE. OK. So, let's talk about the Federal IT Dashboard. It's supposed to give us all the answers. Is it reliable?

Ms. MARTORANA. It is reliable as it is up, running, and operating. But systems are only as good as the data that is input into them, and it is——

Mr. HICE. Exactly. So, where is that data coming from?

Ms. MARTORANA. Federal CIOs. It is their responsibility to enter data into the IT Dashboard on behalf of their agency and their program.

Mr. HICE. But we don't know how accurate that information is.

Ms. MARTORANA. You know, I think going back to my opening statement, talking a little bit about paper, these are manual processes, right? We have—in many technology areas, we've advanced so far. Having machine-readable data, having APIs and automated ways of collecting data, analyzing data, and creating actionable insights from that data, these are all manual data calls that agencies are submitting.

And I say we can do better by investing in some of the tools at agencies so that all of us that have oversight roles are able to make more informed decisions from the data-sets available.

Mr. HICE. Well, I would agree with you that we've got to do more, and we can do more.

Is there—just a kind of a yes or no, because I've got a couple more questions. Is any of that data verified? Is there a third-party independent group verifying the information on the Dashboard?

Ms. MARTORANA. My team spends an enormous amount of time doing that verification. It is one of the reasons that we are oftentimes late in meeting our deadlines is that these are very manual processes that rely on humans looking at the data, finding anomalies, reaching back out to agencies, cleaning that data so that we have a data-set that is more accurate and actionable.

Mr. HICE. OK. So, you bring up your position. And I did have questions with that too, you know, with the ability that you do or do not have to actually produce change. I'm curious about that. And I see my time is running out. So, I'm going give you three

questions that I would like for you to respond back to the committee so that I don't take more than the generous time the chairman has given right now.

But question No. 1: Can you supply this committee with a copy of your job description?

Second, who established that position? How did the process come about that the Federal CIO position was established?

And then, third, do other CIOs recognize this position? And do they, for lack of a better word, submit to your proclaimed authority?

If you could submit an answer to those questions here in the next week or so, I would appreciate it.

Thank you, Mr. Chairman.

Ms. MARTORANA. I'd be happy to. Thank you.

Mr. CONNOLLY. Thank you, Mr. Hice.

And, Mr. Hice, if I could piggyback onto your request, I would add: And what is the relationship between your office and the CTO? How does that work?

Because my recollection is those offices were created by President Obama, and we had Vivek Kundra and Aneesh Chopra from Virginia as the first two holders of those offices, CTO and CIO respectively. And they had a great working relationship.

But to Mr. Hice's point, has it subsequently been more refined and delineated? I assume, of course, it has. So, I think we'd want to know that as well in your responding to Mr. Hice. And if you'll get the answers to the chair, we'll make sure that they are distributed to Mr. Hice and to other members of the subcommittee.

I thank you, Mr. Hice.

Mr. HICE. Thank you, Mr. Chairman.

Mr. CONNOLLY. The chair now recognizes himself for his line of questioning.

Mr. Hice raised the question, and it's a good one. Do you believe that Congress should codify your office, your role in law so that it's not a position that could be dismissed with or abolished by some subsequent executive branch without consultation and consent of Congress and that you'd have statutory standing, obviously, in terms of your roles and responsibilities?

Ms. MARTORANA. IT is such a critical part of how we operate the Federal Government and deliver services. I think that continuing to make sure that C-suites at every agency have capabilities, in addition to the CIO—in my private sector experience, I worked with other executives. While they didn't have the responsibilities that I had, they had a keen understanding and exposure to technology and the problems that we were trying to solve together to support our business or, in the case of government, mission.

So, I think that continuing to focus on IT, Federal IT, and cybersecurity and how we can be best partners, both in supporting agencies doing their mission and our oversight, our critical oversight roles, I think we can continue to improve there. So, I would leave it to the committee to——

Mr. CONNOLLY. Well, I must say I'm biased in favor of codifying things in law because that gives it standing, that regularizes oversight, that empowers people in your job. And all of that's very important, frankly, in a large bureaucracy, both here in Congress and

in the executive branch, as I know you struggle with every day in terms of are you empowered.

And that goes to a different question. One of the—one of the scorecard items we have for FITARA that we added was: Who does the CIO report to? Now, background, before your time, but when we wrote FITARA 7 or 8 years ago, there were—we estimated, among 24 Federal agencies, there were 250 people with the title CIO.

Now you know from your own private sector experience, and mine as well, I mean, generally, corporations have one CIO. The Federal Government as a Federal Government has one CIO, but agencies have multiple CIOs. And that can create confusion and delusion of responsibility and accountability.

So we didn't—we didn't change that in law because we wanted to respect the culture and not be too radical. But we wanted to move toward a primus inter pares, right, that there'd be one primary CIO. And we felt empowerment, just like we're talking about codifying your job, was about reporting sequences, right? We want the primary CIO reporting to the boss.

How do you think we're doing in sort of spreading that word, and how do you think we're doing in terms of evolving a management hierarchy that makes sense from any kind of management point of view, especially given your private sector experience?

Ms. MARTORANA. FITARA has been critical in getting CIOs into the right conversations at the right time. So it—the work of the subcommittee has been mission critical for CIOs.

Each agency has a unique structure, right? There are organizations that have that main headquarter CIO, and then they have component CIOs. So, I really think that it comes down to how technology is thought of as the decision-making process happens in an agency, right? You have to partner with your mission partners, with your program partners from the inception.

So, there are high-functioning agencies that are federated, and there are small agencies that have a single CIO that are also successful. But I think this is an area we can continue to work together on and really improve our overall delivery of IT across the government.

Mr. CONNOLLY. Yes. I—again, we respected the culture. But I will remind you, there are very large corporations that also have many divisions that are disparate, and they have one CIO.

So, we need to guard against the multiplicity of CIOs that contributes to managerial confusion and lack of accountability, at the end of the day. So I—our view is we want to see every primary CIO report to the head of the respective agency because he or she is then empowered, and everyone then knows it.

Let me ask about FedRAMP. Congress, the House, has put a priority on FedRAMP. We've passed FedRAMP legislation five times on a bipartisan basis, five times. The first bill in this Congress—and I managed it—in January right after the insurrection was FedRAMP.

And we continue to hear lots of complaints from the private sector about how FedRAMP, which was designed to be a low-cost, quick, efficient way of being certified to provide cloud services to the Federal Government, is anything but. It's complicated. It's du-

plicative. It forces people to reproduce, you know, documentation, certification processes already approved by some other Federal agency. And it costs a lot of money. And that is a barrier, especially to smaller, more innovative companies that simply can't afford to risk that money, not even knowing if they'll be certified.

Now, that's not how it was supposed to work. And by the way, we talked about codification. FedRAMP is also a creature of the executive branch. It has no basis in statute. And our bill would, of course, change that too, and give it codification in law so that it has standing.

What's your take on what's wrong with FedRAMP and what we can do to try to get it back to its original intent?

Ms. MARTORANA. Yes. I really appreciate your efforts in this area because it is absolutely important to the codification of that program.

We're on a path to really make sure that FedRAMP is the most robust marketplace it can possibly be, but it is not meeting the need today; that, to your point, there are many small companies, there's innovative software that we would love to be able to have go through a FedRAMP program, but it is cost prohibitive for some of these small organizations.

So, we have actually asked members of my team to work collaboratively with GSA and the program team and really roll up our sleeves. We need to fix this to make sure that not only we are supporting the supply chain issues, making sure there's secure software development, but also making sure that we can meet the speed of the need of Federal agencies to have some innovative technology available to them with the umbrella security of the FedRAMP seal of approval in a way.

So I fully applaud that, and we are spending time on that in my office.

Mr. CONNOLLY. So, one of the things I commend to you, you might want to take a look at, we wrote—which I think is absolutely necessary—we wrote a new standard that said presumption of adequacy. So, if you've been approved at one window, Federal window, to provide those services, it is presumed that you have already demonstrated adequacy for other windows.

Now, that doesn't preclude a specialized need, but you shouldn't have to start all over again de novo. I mean, that's part of the problem.

Ms. MARTORANA. Yes.

Mr. CONNOLLY. It's costly, duplicative, and in some cases eliminates people from even trying. And who knows what we're losing as a Federal client, right, from those services.

So, I think that's a very important standard, and my hope is our FedRAMP bill this year, fifth time will be the charm and we'll finally get it into law. But I think it's really important that we do that.

Legacy. I wanted to go back to Mr. Hice's question about legacy. And then my final question will be on TMF.

But I heard your definition of legacy, but I'm not sure I agree with it. I mean, first of all, the word "legacy" implies old, right? I mean, the word has meaning. And so something that's a legacy

comes from the past. And it isn't just "doesn't meet my needs today," because that could be a new system that just doesn't work.

So I think we have to—I think we need to be a little more specific in what legacy means.

Now, let's take IRS. IRS has—they have some systems that use COBOL. And I've talked to people, vendors and some IRS employees, that say, "You know, it still works though. And, I mean, it's good and it's reliable, and we're nervous about replacing it with something new that may not work, or, you know."

But the problem is, over time, a legacy system needs enormous maintenance, it's energy inefficient by definition if it's 40 years old or older, and the number of people who know how to use the language required is dying out.

So, I take the point I think you made, and others have made that, well, you've got to distinguish, they're not all the same, and I agree.

But aren't we concerned that legacy systems by definition bring a lot of inefficiency, they're costly and they're risky, because not only can they break down and thus our constituents are not served, but they're also hackable, right? Not all of them are easily encrypted and protected.

And so moving to a new generation of technology to replace old legacy mainframes really ought to be a general goal, not a mindless goal but something we push pretty hard.

What is your view about that point of view?

Ms. MARTORANA. Legacy is—it's a tough subject. We should be operating the United States Federal enterprise on the most modern technology available, full stop. If we are going to deliver digital transformation for the American people in our lifetimes, we have got to improve the foundational cybersecurity as well as operating presence of our technology.

That takes investment over, you know, years and years for us to get out of this tech debt that we have across almost every single agency.

I did a mainframe migration project when I was at OMB. We had mainframes at risk in a subbasement. The challenging part was, we weren't able to recognize the cost savings as quickly as I would've hoped in my private sector experience.

So you had to start, first reengineer all your business processes, because you can't just lift and shift and do exactly what you did on the mainframe without interrogating the way that you do business, because newer systems are differently efficient, and they potentially have the opportunity for us to really leapfrog.

So, you want to make sure that you're thinking about the business process and not just moving old, antiquated, because that's the way we did it 25 years ago, to the cloud, for example. You want to interrogate all of that along the way.

But I had originally planned, once we were able to get the new mainframes up and running that were cloud ready, doing all of the steps that we needed. I thought we would be able to sunset the old equipment. So, get rid of operations and maintenance cost and all of the ancillary costs and staffing that had to be burdened managing those systems instead of moving up with the new systems.

It took years of compliance activity that we needed to go through in order to actually get those offline and stop paying for both. So, we were really challenged in recognizing cost savings.

And I think that would be something it would be really worthwhile for us to partner together on interrogating, going through some of the programs that we've seen do this very efficiently and other ones maybe that took a little bit longer and see if we can come up with some best practices and really share them more widely across the Federal enterprise.

Mr. CONNOLLY. So, I think you've done a great job setting the goal about legacy. That's clear and unambiguous, and I think that's a good new standard—or maybe it's not so new, but it's declaratively stated. So thank you.

And just my final—and I don't mean to impose on time—but I just wanted to clarify some things that Mr. Hice and others have raised.

TMF, the Technology Modernization Fund, was directly related to this whole question of retiring legacy systems and upgrading technology. Is that correct?

Ms. MARTORANA. That is correct.

Mr. CONNOLLY. And we provided a billion dollars and we celebrated that. Is that correct?

Ms. MARTORANA. Correct.

Mr. CONNOLLY. However, replacing a big system at a Federal agency could be multiyears and multibillions of dollars, just that one system or that one agency. Is that correct?

Ms. MARTORANA. Absolutely.

Mr. CONNOLLY. So, a billion dollars is great in incentivizing people to—and here's the—why do we need—because Mr. Hice raised this question, it's a fair question—why do we need extra money? We're spending almost $100 billion a year in IT that we know of, maybe more. Why do you need more money to incentivize agencies to retire their legacy systems?

Ms. MARTORANA. Yes. TMF was really—the billion dollars for TMF was a down payment. The three years prior to the American Rescue Plan, the last year, TMF only saw one proposal. So, obviously something wasn't meeting the need of agencies if only one agency came forward with an IT modernization project for TMF.

So, the billion-dollar down payment on kick-starting—re-kick-starting TMF gave us the opportunity to really rethink the way that we were thinking about our projects and funding them.

And in addition, the payment flexibility gave us the opportunity, it allowed agencies not to self-select out. Many of them selected out of the original TMF because of what we just spoke about with cost savings taking longer to recognize.

So, I think that we're on a really good path to showing significantly improved outcomes on the programs, and I really hope that we continue to get the investment, because we are standing up something that is going to be transformative. It's a catalyst in helping agencies get started on some of these complicated projects.

Mr. CONNOLLY. Mr. Hice, I see you're still on. If you want to jump in at this point, take a few minutes to either ask additional questions or comment. I certainly want to be fair to you. So you're recognized.

Mr. HICE. Thank you very much, Mr. Chairman. I was going to ask if I could have just a couple more minutes.

Ms. Martorana, during our hearing in May on TMF, Congressman Biggs observed that in order to perform appropriate oversight this committee needs access to certain written agreements between agencies regarding the Technology Modernization Board; quite frankly, things like reimbursement requirement schedules, status of repayments. In fact, quite frankly, I think all of these things should be publicly available.

So let me just ask you: As chair of TMF Board, will you commit to providing this committee with that type of information and, quite frankly, even make that information publicly available?

Ms. MARTORANA. Thanks for that question.

I believe GSA, in response to the May hearing, did provide everything that was requested by the committee. So, I will followup. I'm happy to followup with my colleagues at GSA about that.

We are working on——

Mr. HICE. Will you make that information available?

Ms. MARTORANA. We are working to upgrade the TMF website so that we can continue to be more transparent about the investments that we are making. So, I do commit to us working on publishing out some of that data on the TMF website. But happy to——

Mr. HICE. OK. My question is really twofold. I'm not asking for some of that information, but all of that information, first of all, to this committee, and second, publicly. But primarily, to begin with, this committee needs access to that information.

Ms. MARTORANA. I absolutely will commit to us being as responsive to Congress as we should be and provide you, the committee, what you need.

As far as——

Mr. HICE. No, no, no. Listen, I don't want you determining what we need. I want this information, and I'm asking you to provide it.

Ms. MARTORANA. And I'm concurring that I am agreeing with you and will provide the information that you have requested. It was my understanding GSA had already done that. So full stop——

Mr. HICE. OK. Thank you. Thank you very much for your help with that.

And my last real question. Cybersecurity is a notoriously decentralized issue in the Federal Government with various senior-level officials playing very important roles. We've seen the National Cyber Director, Chris Inglis, for example, and CISA Director Jen Easterly, just to name a couple.

But now, with you as the Federal CIO, do you have a substantive seat at the table when it comes to protecting our Federal agency information systems? That to me is a very important issue.

And if you do have a table there, what are your responsibilities? What does that consist of? What is your relationship with other IT-related cybersecurity offices and officials? That type of thing.

Ms. MARTORANA. Thanks for the question.

The National Cyber Director is the principal adviser to the President on cybersecurity policy and strategy. I am responsible for overseeing Federal cybersecurity programs and ensuring that they align with the national cyber directive strategy.

The Federal Chief Information Officer, Mr. Chris DeRusha, who is on my team, is also a deputy in the National Cyber Director Office for Federal cybersecurity.

This is an area where we have worked really closely in the last year, since the National Cyber Director Office has been stood up, to work collaboratively across the executive branch, and we work really closely with the CISA team.

And I feel like we—this is an area—you've probably heard that—many of us say that cybersecurity is a team sport. This is a team sport where I feel like we are winning as collaborators.

We still have risk to our Federal Government, but I think in this specific area the National Cyber Director role has been critical, and we have been very successful at working to safeguard the Federal enterprise by working so collaboratively with CISA, the National Cyber Director, and——

Mr. CONNOLLY. Thank you.

And I thank the gentleman.

Mr. HICE. So, do you have a seat at the table?

Ms. MARTORANA. Absolutely. And my—Federal CISO is dual-hatted to the—on to the National Cyber Director team. So, we not only have—I not only have a seat at the table, we work together every single day in that dual-hat role to make sure our teams are completely coordinated.

Mr. CONNOLLY. So thank you, Mr. Hice.

Mr. HICE. Thank you, Ms. Martorana.

And, Chairman, if I could just kick it back to you, but say thank you again for hosting this hearing and for leading us in this.

This is an extremely complex discussion. All of us realize that cybersecurity is a major issue that must be addressed.

I think collaboration, it is one thing. We've got to get beyond that. We've got to address the problems. We've got to get rid of legacy systems. We've got to improve this. We've got to have accountability.

And, Ms. Martorana, I look forward to having further discussions with you, and we'll look forward to doing that.

Mr. CONNOLLY. Thank you, Mr. Hice, and I certainly agree with you about accountability.

Let me also at this juncture, before I call on the gentleman from California, I have one, two, three, four, five, six, six memos from OMB that provide guidance on cybersecurity dating back to August 2021. And I would insert them in the record at this point.

I would also insert into the record the GAO guidance with respect to reimbursement we discussed a little earlier on TMF.

Without objection, so ordered.

Mr. CONNOLLY. We've been rejoined by the gentleman from California, Mr. Khanna.

Mr. Khanna, you are recognized for your five minutes of questioning, and we're going to be generous in that five minutes if you need it.

Mr. KHANNA. Thank you, Chair Connolly. I will try to be brief. You continue to show exceptional leadership on everything concerning technology in our government.

I particularly appreciate Ms. Martorana as the head of IT in appearing. And your strong and thoughtful leadership and your time

in government make our government more technologically savvy and proficient.

I've been discussing with the chair and with many people at the White House, senior leaders, about the creation of a Federal chief customer experience officer or an equivalent position directed to improve government service.

The White House is very excited about the idea. They recognize, President Biden and others have, that it's more than customer experience. It's about more than technology. It's about making sure that we are serving people.

And that's been the secret to a lot of Silicon Valley's success. It's about making sure that the community is working together, that we have the right mail and telephone services.

So, Ms. Martorana, I just want to make sure we have your commitment, which I imagine we will, on working on this to make it a success and make sure we can get this win for President Biden.

Ms. MARTORANA. If anyone knows anything about me, they know that customer experience is—has been what I've spent the majority of my career working on, making sure that we are delivering the right products and services to the people that need them and that they can engage with them seamlessly regardless of their abilities. It is absolutely the cornerstone of what we work on.

It's also really a critical third—if you think of cybersecurity as the foundation, IT modernization and customer experience, they all work together in IT. I have never worked on a successful project that did not think of all of the dimensions both——

Mr. KHANNA. Terrific. So, I just wanted—so you'll work with us then on this legislation on the Federal chief customer experience officer. We've been working with folks at the White House on it, but I want to make sure, since you're integrally involved, that we can have your help with it as well.

Ms. MARTORANA. I'd be happy to join any conversations related to it.

Mr. KHANNA. Thank you. Well, we'll look forward. I appreciate your commitment to support it and work on it, and really appreciate your leadership, and our team will be in touch. And the chairman has been extraordinary on this.

Thank you very much.

Thank you, Mr. Chair.

Mr. CONNOLLY. Thank you, Mr. Khanna, and I hope I can quote you in all of that praise.

All right. Thank you for joining us today. And thank you for championing customer experience, because I think that's very important. And, in fact, I'm proud to be a cosponsor of the Federal Agency Customer Experience Act. So, we'll be talking about that as well.

In closing, I want to thank Ms. Martorana for joining us. I want to commend my colleagues for their diligence and their dedication to this set of issues.

It doesn't make headlines. It's not sexy. Everything hinges on technology. Everything. All of our programs, all of our aspirations, all of our goals, all of our objectives, all of our noble purposes rise or fall on the IT platform ultimately and its security. And those are

investments critical to the American people and for our mission. So thank you.

Without objection, all members will have five legislative days within which to submit additional written questions for the witness. And I would ask that those questions come through the chair and the answers come through the chair.

Mr. Hice gave you three questions that he would like answered and I modified one of them. And if you need us to put that in writing, we will; or, if you don't, if you could just try to get back to us, I would very much appreciate that.

And thank you again for joining us today.

And thank you to my colleagues and our staff.

And with that, this hearing is adjourned.

[Whereupon, at 10:28 a.m., the subcommittee was adjourned.]