

**FEDERAL IT MODERNIZATION:
HOW THE CORONAVIRUS EXPOSED
OUTDATED SYSTEMS**

HEARING

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT OPERATIONS
OF THE
COMMITTEE ON OVERSIGHT AND
REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JULY 20, 2020

Serial No. 116-104

Printed for the use of the Committee on Oversight and Reform



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

U.S. GOVERNMENT PUBLISHING OFFICE

41-183 PDF

WASHINGTON : 2020

COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

| | |
|---|---|
| ELEANOR HOLMES NORTON, District of Columbia | JAMES COMER, Kentucky, <i>Ranking Minority Member</i> |
| WM. LACY CLAY, Missouri | JIM JORDAN, Ohio |
| STEPHEN F. LYNCH, Massachusetts | PAUL A. GOSAR, Arizona |
| JIM COOPER, Tennessee | VIRGINIA FOXX, North Carolina |
| GERALD E. CONNOLLY, Virginia | THOMAS MASSIE, Kentucky |
| RAJA KRISHNAMOORTHY, Illinois | JODY B. HICE, Georgia |
| JAMIE RASKIN, Maryland | GLENN GROTHMAN, Wisconsin |
| HARLEY ROUDA, California | GARY PALMER, Alabama |
| RO KHANNA, California | MICHAEL CLOUD, Texas |
| KWEISI MFUME, Maryland | BOB GIBBS, Ohio |
| DEBBIE WASSERMAN SCHULTZ, Florida | CLAY HIGGINS, Louisiana |
| JOHN P. SARBANES, Maryland | RALPH NORMAN, South Carolina |
| PETER WELCH, Vermont | CHIP ROY, Texas |
| JACKIE SPEIER, California | CAROL D. MILLER, West Virginia |
| ROBIN L. KELLY, Illinois | MARK E. GREEN, Tennessee |
| MARK DESAULNIER, California | KELLY ARMSTRONG, North Dakota |
| BRENDA L. LAWRENCE, Michigan | W. GREGORY STEUBE, Florida |
| STACEY E. PLASKETT, Virgin Islands | FRED KELLER, Pennsylvania |
| JIMMY GOMEZ, California | |
| ALEXANDRIA OCASIO-CORTEZ, New York | |
| AYANNA PRESSLEY, Massachusetts | |
| RASHIDA TLAIB, Michigan | |
| KATIE PORTER, California | |

DAVID RAPALLO, *Staff Director*
WENDY GINSBERG, *Subcommittee Staff Director*
AMY STRATTON, *Clerk*

CONTACT NUMBER: 202-225-5051

CHRISTOPHER HIXON, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

| | |
|---|--|
| ELEANOR HOLMES NORTON, District of Columbia | JODY B. HICE, Georgia <i>Ranking Minority Member</i> |
| JOHN P. SARBANES, Maryland | THOMAS MASSIE, Kentucky |
| JACKIE SPEIER, California | GLENN GROTHMAN, Wisconsin |
| BRENDA L. LAWRENCE, Michigan | GARY PALMER, Alabama |
| STACEY E. PLASKETT, Virgin Islands | RALPH NORMAN, South Carolina |
| RO KHANNA, California | W. GREGORY STEUBE, Florida |
| STEPHEN F. LYNCH, Massachusetts | |
| JAMIE RASKIN, Maryland | |

C O N T E N T S

| | |
|---|-----------|
| Hearing held on July 20, 2020 | Page 1 |
| WITNESSES | |
| Gordon Bitko, Senior Vice President of Policy, Information Technology Industry Council Oral Statement | 6 |
| Matthew Cornelius, Executive Director, Alliance for Digital Innovation Oral Statement | 7 |
| Steve O’Keeffe, Founder, MeriTalk Oral Statement | 10 |
| Hana Schank, Director of Strategy, Public Interest Technology, New America Oral Statement | 11 |
| <i>Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.</i> | |

INDEX OF DOCUMENTS

Documents entered into the record during this hearing and Questions for the Record (QFR’s) are available at: docs.house.gov.

- * Questions for the Record: to Mr. Gordon Bitko; submitted by Chairman Connolly.
- * Questions for the Record: to Mr. Matthew Cornelius; submitted by Chairman Connolly.
- * Questions for the Record: to Mr. Steve O’Keeffe; submitted by Chairman Connolly.
- * Questions for the Record: to Ms. Hana Schank; submitted by Chairman Connolly.
- * Questions for the Record: to Mr. Gordon Bitko; submitted by Rep. Jody Hice.
- * Questions for the Record: to Mr. Matthew Cornelius; submitted by Rep. Jody Hice.
- * Questions for the Record: to Mr. Steve O’Keeffe; submitted by Rep. Jody Hice.
- * Questions for the Record: to Ms. Hana Schank; submitted by Rep. Jody Hice.

**FEDERAL IT MODERNIZATION:
HOW THE CORONAVIRUS EXPOSED
OUTDATED SYSTEMS**

Monday, July 20, 2020

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

The subcommittee met, pursuant to notice, at 1:38 p.m., in room 2154, Rayburn House Office Building, Hon. Gerald E. Connolly (chairman of the subcommittee) presiding.

Present: Representatives Connolly, Norton, Plaskett, Khanna, Lynch, Raskin, Hice, Massie, Grothman, Norman, Steube, and Comer (ex officio).

Mr. CONNOLLY. The hearing will come to order, and I welcome everybody to this hybrid hearing. Both Ranking Member Mr. Hice and myself have wanted to have hearings resume in person, especially when we are in session, and I made a promise to Mr. Hice that I would fight for that, and today is the fruit of that effort.

I believe when we're in session, to the extent possible, protecting everybody's health and safety, we can and should be meeting like this in at least hybrid form. Those members who are not comfortable or physically cannot join us in the hearing room are more than welcome to join us through webinar, and we're happy to have them.

We ask everybody, when they are not speaking, to wear a mask. That is the guidance of the Capitol Hill Physician, that is the guidance of the chairwoman of this committee, and it protects everybody. I really appreciate that cooperation.

Let me see. For members appearing remotely, just a few reminders before I give my opening statement. House rules require that we see you. So, please have your cameras turned on at all times during the course of the hearing. Members who are not recognized should remain muted so we minimize background noise and feedback.

I'll recognize members verbally, and members retain the right to seek recognition, if they can let us see through either our staff or have your staff contact our staff, and we'll be glad to try to make sure you get recognized. You can use the chat function to send a request. And if none of all that works, you can unmute your mic and seek recognition.

We're going to try to minimize, obviously, people talking over each other.

These aren't ideal circumstances, but we are in the midst of a pandemic that, tragically, is growing rather than contracting, and so we want to make sure we are safe. A number of our colleagues and staff members, Capitol Hill Police, have come down with the virus, and we don't want to do anything unwittingly that could spread that contagion. So, we will do everything we can to try to make sure this is a safe environment in which to operate.

With that, I recognize myself for my opening statement.

The Federal Government's response to the pandemic has exposed some fundamental weaknesses that have to be fixed, especially legacy IT systems. Throughout this global health crisis, millions of Americans facing illness, unemployment, food insecurity, and an inability to pay their mortgages or rent have looked to the Federal Government for help.

Yet despite urgent congressional action that provided unprecedented levels of economic assistance, those in need have often had their misery exacerbated by broken IT infrastructures at the Federal and state level that have prevented them from receiving timely support.

The CARES Act, which was overwhelmingly passed on a bipartisan basis by this Congress, was signed into law on March 27. It is now July 20. We still do not have the full postmortem on the failures of the Small Business Administration E-Tran system tasked with facilitating more than \$750 billion dollars in small business loans and grants. The Internal Revenue Service has yet to deliver tens of millions of economic impact payments. And in my home state of Virginia certain types of unemployment claims will not be available until August due to the state's failure to update its IT systems.

The public policy was there, but our IT systems often couldn't deliver. In other words, the fate of the world's largest economy rises and falls often with the ability of government IT systems to deliver in an emergency, and that should galvanize us all.

It has been reported that 21 million people were unable to receive their CARES Act stimulus payments because IRS could not find accurate direct deposit information. Hundreds of thousands of small businesses were shut out of SBA's system for submitting loan applications. And for every ten people who successfully filed for unemployment, an additional three to four were unable to submit claims online. That's a big problem when we're looking at 31 million people on an ongoing basis who depend on the unemployment check every week.

Issues with legacy IT systems are not news to us on this committee. We enacted the Federal Information Technology Acquisition Reform Act, FITARA, of which I was a proud co-author, to help Federal agencies prioritize Federal IT modernization.

And the Modernizing Government Technology Act, also coming out of this committee, was passed to enable agencies to establish working capital funds to help them use savings from IT modernization in order to further invest in upgraded agile systems and transition away from those legacy systems, legacy systems that are often 30 and 40 years old.

The law also created, coming out of this committee again, the Technology Modernization Fund, which established a government

funding source for agencies to remove and replace those legacy systems and upgrade their own. Yet the TMF remains chronically underfunded, and outgoing Chief Information Officer Suzette Kent has identified this underfunding as illustrative of the small-bore thinking that, unfortunately, has prevailed when it comes to making IT investments.

Agencies responsible for performing critical government functions operate on legacy systems with components sometimes dating back even 50 years.

The Government Accountability Office found that the ten most critical Federal IT legacy systems in need of modernization are maintained by ten different Federal agencies, each performing essential government operations. As they age, these legacy systems become more expensive to maintain, more vulnerable to cyber-attacks, less effective in accompanying agency missions.

If FEMA's public alert and warning system fails, millions of lives could be lost during a natural disaster because life-saving information was not delivered to the public in time. If the Department of the Interior system that monitors power plants stalls, thousands of communities could be left without power.

Simply put, outdated and inefficient systems put American lives, as well as livelihoods, at risk.

As we heard from organizations representing Federal workers in a subcommittee hearing two weeks ago, agencies have been able to leverage telework to ensure the continuity of government operations, while also protecting the health and safety of Federal workers. Nonetheless, the large-scale shift to telework exposed critical cybersecurity vulnerabilities underlying that outdated IT.

Since the pandemic hit, IGs, inspectors general, have reported increased risks of data security breaches, disclosures of classified information, and targeted cyber-attacks and fraud schemes affecting financial aid to small business and people affected by the pandemic.

Going forward, Federal agencies will need to quickly retire their legacy systems and prioritize modernizing IT, like adopting cloud computing technologies through FedRAMP, a program that enables agencies to quickly secure and adopt new technologies. And I'm grateful for the fact that in the defense authorization bill we're considering today on the floor, in the first en bloc group of amendments our FedRAMP bill that came out of this committee is included.

In 2019, 13 agencies reported to GAO that they achieved at least \$291 billion in savings from increasing their investments in cloud technologies. I hope we can continue to advance the bipartisan FedRAMP Authorization Act that passed the House by voice vote into law and signed by the President on a bipartisan basis.

Modern, reliable IT is not just a nice thing to have. Our Federal Government's consistent failure to prioritize IT modernization and program delivery prevented the public from receiving the assistance Congress authorized to help the Nation weather one of the worst global pandemics in a hundred years. We can no longer allow outdated, legacy technology to stymie the delivery of vital public services. We will need to rip out root and stem systems that have hung around for decades because the replacement costs have been

prohibitively expensive, because if doing so is a matter of being able to save the American economy from collapse, almost anything is cheap by comparison.

With that, I call upon the distinguished ranking member for his five-minute opening statement.

Mr. HICE. Thank you very much, Mr. Chairman. I appreciate a great deal you working with us to make this hearing happen. I really am grateful for that.

I would say, though, that guidance to wear masks are one thing and committee rules are another. There's no question that in this room right here we are well beyond the guidance that the CDC recommends, and we have had some who are not here today because they feel as though we are too strict in the requirement of the mask.

So, I would ask as we go forward that we would continue to work through this to see how we can accommodate all members who would like to participate in hearings within the CDC guidelines as well.

Mr. CONNOLLY. I will, as I have on having a hearing physically, as my friend knows, I will work as diligently as I can with him. I will, however, note that the committee is following the guidance of the Capitol Hill Physician, who more than strongly recommends the wearing of a mask. It isn't just CDC guidance.

So, we will try to work through that with you. And I really appreciate all of my colleagues trying to respect everybody's health and safety today.

Mr. HICE. Right. I know you will, and I look forward to those further conversations. But on behalf of others who feel a little bit differently, I would appreciate that continued conversation. Thank you very much.

I also appreciate, Mr. Chairman, the fact of you holding this particular hearing on Federal IT modernization. I think we are all very much aware of the need for modernization in this area. The lack thereof certainly exposes us to security risks, as well as the inability for flexibility and scaling up.

Ultimately our agencies were incapable of meeting the needs and the responsibilities they are required to do, and yet we, as a government, continue to spend the majority of our budget on maintaining these legacy systems rather than taking us into the new era of computer needs.

For example, from 2010 to 2017, over \$450 billion was spent just to keep legacy systems running. Of course, that also represents \$450 billion that was not able to be used for new technology. And at the same time, of course, technology continues to move forward and improve while we are slow to procure any new capabilities whatsoever.

So, it's time for us to look at reform. It's time for us to look at changes. How do we go about getting up to date? There's no reason that we don't do so.

I very much look forward to our witnesses today and appreciate you being here as we try to consider ways to reform the IT acquisition process and to prevent agencies from trying to reinvent the wheel, particularly when potential solutions already exist in the commercial marketplace.

So, specifically this committee is interested, I believe, in learning how and what Congress needs to do to help agencies overcome some of the challenges that are presented by annual funding cycles that, frankly, makes it very difficult to tackle as it relates to IT modernization.

I'm hoping today that our witnesses will be able to help this committee understand how we can improve this whole process, and particularly the Technology Management Fund, to help the government replace limited systems. We've got to become more modern and up to date rather than continuing to rely upon agile old systems.

Finally, I think there's got to be some accountability in this whole process to keep agencies responsible for the progress that they are making. Of course, there have been many hearings we've already had on the FITARA Scorecard. Somewhere along the way, though, there must, it appears to me, be some sort of incentive that must be involved to help agencies come along and to improve.

So, I look forward to hearing all these types of things as we move forward with the hearing today, and I'm hopeful that you will be able to supply some of those answers. I want to, again, thank all of our witnesses for being here today as we participate in this hybrid hearing.

Mr. Chairman, with that, I'll yield back.

Mr. CONNOLLY. I thank my friend, and he makes some really good points.

By the way, our next FITARA hearing is Monday. It is the tenth hearing we will have had on the implementation of FITARA. And the good news is, I think, for the first time since we passed the bill, there are no F's and no D's in the scorecard. So, we've made some progress. But we've still got to retire those legacy systems you were talking about, and that's going to require some finesse.

So, I thank the distinguished ranking member.

I would like to introduce our witnesses. Our first witness today is Gordon Bitko, who is senior vice president of policy for the Information Technology Industry Council.

We're also joined by Matthew Cornelius, who is here physically, who's the executive director of the Alliance for Digital Innovation.

We'll also hear from Steve O'Keeffe, the founder of MeriTalk and somebody who actually was the inspiration for the FedRAMP legislation and has done a lot to try to translate the FITARA Scorecard into more digestible ways that I think have been very helpful.

Our final witness will be Hana Schank, who's the director of strategy for New America.

If our three witnesses who are remote and Mr. Cornelius, if you would rise and raise your right hand. It is the practice of our committee to swear in our witnesses. And if the other three witnesses can raise their right hand? All of you confirm you are doing so?

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

Let the record show that the witnesses have indicated in the affirmative.

Thank you.

Without objection, written statements will be made a part of the record. We ask all of our witnesses to try to summarize their testimony within the five-minute time limit.

With that, Mr. Bitko, you are recognized for your testimony.

**STATEMENT OF GORDON BITKO, SENIOR VICE PRESIDENT OF
POLICY, INFORMATION TECHNOLOGY COUNCIL**

Mr. BITKO. Good afternoon, Chairman Connolly, Ranking Member Hice, and distinguished members of the subcommittee. Thank you for inviting me to testify today. It is a privilege to discuss Federal IT modernization issues with you.

My name also Gordon Bitko, and I'm the senior vice president for public sector policy at ITI, the Information Technology Industry Council. Previously, I was the CIO at the FBI for 3-1/2 years, and I have more than 25 years of experience as a technologist and technology manager across the public and private sectors.

ITI represents more than 70 leading IT companies who believe it is more important than ever for the U.S. Government and our member companies to work together in support of policies that promote effective government through technological leadership.

The U.S. public sector must leverage this innovation and leadership by adopting policies that enable easier use of commercial products and services that provide security, agility, scalability, and elasticity that support the enormous growth in demand for digital services and data.

That imperative to modernize is true at every government agency, and the ongoing pandemic, with the vast increase in remote work, has only accelerated the need for change.

The ability for Federal agencies to shift to large-scale telework during the pandemic is the result of some of the transformative activities of recent years, such as migration to commercial providers for at least some critical infrastructure and services.

But incremental change is insufficient in the face of exponential growth. When stressed enough, legacy systems fail catastrophically. We saw this in multiple state unemployment systems, but many Federal agencies also provide critical services through decades-old systems.

Providing the quality of service that Americans expect and deserve means these systems must modernize. Technological transformation can only happen if there's consistency and a dedication to both providing funding and addressing the policies and practices that restrain innovation and modernization in government information technology.

The Department of Justice Data Center Consolidation Initiative highlights many inhibitors of innovation. Starting in 2014, DOJ planned to consolidate to three core facilities with two owned and operated by the FBI, including a newly funded center constructed at an existing facility in Idaho. An RFP was posted in February 2016, groundbreaking occurred in October 2017, the building opened last November, and full operation is scheduled for this September.

It will already be out of date. Two years ago, commercial providers consulted about providing services using the facility declined. It already fell short of their technical requirements.

A new facility enabling DOJ to close multiple data centers is progress. Data center metrics will improve and some applications will modernize. But it will never be a state-of-the art facility and will continue to host legacy systems subsisting on O&M budgets.

Meanwhile, systems able to invest in modernization will migrate to commercial providers with innovative technologies and resources that dwarf DOJ's.

The government's limited technical and contract expertise, risk aversion, process inefficiencies, unpredictable funding, and inflexible construction processes all contribute to timelines much longer than commercial best practices. At the same time, the lack of multi-year IT modernization funding means that legacy applications endure.

Federal IT isn't held together by duct tape. There are excellent professionals throughout government delivering quality information technology capabilities. But the reality is, it is still too hard for them to get to the front lines and focus on core long-term agency challenges.

When government has defined unnecessarily complex requirements based on data business processes, the overhead of a customized solution has often made projects late, over budget, and underused.

But when the government has well-defined objectives and smartly engaged with industry, the result has been successful and cost-effective commercial services securely provided at speed and scale.

Adopting this approach empowers industry to create world class services for government, drive competition by leveraging standards, and encourage innovation by opening markets to new companies, products, and services.

At the same time, IT budget and acquisition processes must evolve to allow and empower the Federal work force to leverage commercial capabilities.

Transformational change requires long-term strategic and financial commitments. The annual budget cycle forces agency IT planning staffs to spend too much time managing the budget process and too little time ensuring projects and programs are well managed and well funded.

However, those same IT planning staffs need to adopt a continuous delivery mindset. They shouldn't be managing projects on traditional schedules but rather on outcomes, like the delivery capabilities that improve the mission and their use, both within and outside the agency. And government processes and tools for managing IT investments, such as the FITARA Scorecard and the Federal IT Dashboard, need to be updated to reflect those modern realities of IT development.

Thank you again for inviting me, and I look forward to your questions.

Mr. CONNOLLY. Thank you very much.

Mr. Cornelius, you're recognized for five minutes.

**STATEMENT OF MATTHEW CORNELIUS, EXECUTIVE
DIRECTOR, ALLIANCE FOR DIGITAL INNOVATION**

Mr. CORNELIUS. Chairman Connolly, Ranking Member Hice, and distinguished members of the subcommittee, thank you for the op-

portunity to testify today on the vitally important topic of Federal IT modernization.

My name is Matthew Cornelius, and I'm the executive director of the Alliance for Digital Innovation. We're a nonprofit organization made up of nearly two dozen of America's leading commercial technology companies which focuses on empowering the government to deliver the effective digital experiences that citizens deserve.

Our companies have a successful track record of modernization in large, complex enterprises across both the public and private sector. And we at ADI are keenly aware that the government's continued reliance on outdated, insecure legacy technology fundamentally obstructs the creation of a modern, secure digital government.

Today I will share our perspective on both the challenges and opportunities agencies face and will offer some recommendations to improve the speed, scale, and likelihood of success in modernizing legacy IT.

Prior to ADI, I had the privilege of serving in senior Federal IT policy roles in both the Office of Management and Budget and the General Services Administration, where I led the creation and execution of several key governmentwide technology efforts, including the IT Modernization CAP Goal and the President's Management Agenda, and the Technology Modernization Fund. I highlight these additional experiences as I believe they provide me with a unique understanding of IT modernization I can share with you today.

When I describe the government's legacy problem, I want to note that it goes far beyond certain systems that are decades old. It is a cultural problem both inside government and out.

For starters, the government is averse to market pressures and often relies on a woefully outdated business model that prioritizes building and owning technology solutions inside agencies.

In addition, there is little alignment of agency procurement and financial management processes to commercial best practices, and agencies rarely have the appropriate incentives to modernize effectively and partner with truly innovative companies to drive mission outcomes.

The recent report by the Pandemic Accountability Committee highlighted IT and cybersecurity as two major challenges faced by agencies during the response to COVID-19. However, the report also pinpointed numerous examples, such as the Department of Health and Human Services, the Nuclear Regulatory Commission, and the Department of Defense, who have been able to deal with the significant disruptions of COVID-19 because they were already investing significantly in cloud computing and had enhanced both their telework capabilities and digital workflows.

Such examples are possible because these agencies had a commitment to IT modernization from senior leadership, a work force able to effectively buy and deploy these new technologies, and a culture that embraces innovation.

Still, more can be done. A second key to empowering and accelerating IT modernization is to ensure that agencies can easily and effectively acquire and use commercial capabilities to achieve mission outcomes.

While some public sector agencies are embracing cloud and other emerging technologies, too many are hamstrung by technical debt and procurement paradigms that lead to wasteful spending and poor customer satisfaction.

ADI has written extensively on the need for government to follow current law, such as the Federal Acquisition Streamlining Act, which establishes a commercial-first framework. Government must prioritize the acquisition of commercial off-the-shelf solutions, which are easier to embed across the agency's IT enterprise, are more secure, and cost substantially less than bespoke agency-specific systems.

Third, successful IT modernization requires many years of sustained investment and the ability of agency leaders to make adjustments and address challenges that occur along the way.

Unfortunately, the budgeting and appropriations processes rarely provide the necessary flexibility to drive true digital transformation. The current model restricts the ability of agencies to both plan and invest wisely in modernization.

The expansion of IT Working Capital Funds, as envisioned under the MGT Act, would allow agencies to make smarter long-term investments. Additionally, ADI supports providing significantly more money to the Technology Modernization Fund so the government can support digital transformation across the Federal enterprise.

Finally, there are several options Congress may consider to help accelerate IT modernization. For example, Congress should overhaul decades-old laws, such as Clinger-Cohen and the E-Government Act, to provide a current sustainable foundation for IT modernization more aligned to today's technology environment.

Congress should also build on its oversight successes made possible by the FITARA Scorecard to update current metrics and include new ones, such as cloud adoption, FedRAMP authorization and reuse, and the acquisition of commercial items.

Additionally, Congress can continue encouraging agencies to prioritize training the Federal work force on current procurement, cybersecurity, and digital capabilities. Modernization is impossible without a highly skilled, capable work force.

Most importantly, Congress should continue to make IT modernization a critical issue that unites both parties, both Chambers of Congress, and both the legislative and executive branches.

In conclusion, IT modernization is vital not only because it saves money and enhances cybersecurity, it is the primary means for agencies to competently and capably deliver important citizen services to the American people.

ADI is proud to highlight the modernization successes happening across the Federal enterprise and to share our insights on eliminating costly, wasteful legacy IT.

Thank you again for the opportunity to appear here today. I look forward to your questions.

Mr. CONNOLLY. Thank you very much, Mr. Cornelius. I can assure you every single major vote on this committee, since I have been here, on this subject has been bipartisan. We have never had a partisan vote. In fact, it would be hard to tell the difference between us when we start talking about it. So, I'm very proud of that.

Mr. O'Keeffe, you're recognized for five minutes.

STATEMENT OF STEVE O'KEEFFE, FOUNDER, MERITALK

Mr. O'KEEFFE. Thank you.

Chairman Connolly and distinguished members of the subcommittee, thank you for the opportunity to speak today. And, Chairman Connolly, thank you for your constant leadership on Federal IT and work force issues.

My name is Steve O'Keeffe, and I'm the founder of MeriTalk, the leading government IT publication, research, and conference company.

We are here for one reason: The pandemic made the Federal community—and, yes, Cabinet secretaries—and, for that matter, the American public—get the importance of Federal IT. It's Rodney Dangerfield and Winston Churchill here. "We don't get no respect." And as Churchill famously told us, "Never let a good crisis go to waste."

A quick ironic flashback. I testified on this very topic, the urgent need for speed in Federal IT modernization, a decade ago on the Senate side. I testified against then Federal CIO Vivek Kundra, who put forth a 25-point plan to modernize Federal IT. I argued that it was far too complex. There are only Ten Commandments. How can there be 25 points in the plan to fix Federal IT? And it proved true.

Complexity is the No. 1 issue of Federal IT modernization. So, what to do? Well, this is like a five-minute Hamlet, so let's bid the players make haste.

Act 1, attack complexity. The time is right for FITARA and MGT to shine. Moreover, these light house laws and Federal CIOs are mired in the slings and arrows of complexity. We need to cut to the quick.

Consider that complexity. It really is an alphabet pea soup. We have FITARA. We have MGT. We have TMF. We have FedRAMP, DCOI, CoEs, CAP Goals. And I am just scratching the surface. This is madness.

Let's just look at cybersecurity. It's CDM, TIC, FISMA, Einstein, and now DHS gives us QSMO. Even Einstein could not fathom all of that.

How about we simplify and rebrand these initiatives and give them names that describe the function they perform and fit them together into a coherent narrative that explains the value they deliver? And what about we plug those programs all into FITARA with tangible outcomes and metrics associated.

So, first off, let's attack complexity.

Second, FITARA for the future, it's time to evolve. As we approach the 10.0 FITARA Scorecard, which I guess is coming out next week, the legislation has proved a huge success. So, congratulations.

But five years is an eternity in the IT space, and it's time to modernize FITARA. Let's make the FITARA Scorecard real-time, plugging the scoring criteria into the IT Dashboard, and let's make the FITARA IT Dashboard the "to be or not to be" of Federal IT. This would kill confusion about what's measured in FITARA and make FITARA the real-time epicenter in a radically simplified Federal IT government landscape.

And as in Shakespeare's plays, relationships are very important. We need to wed FITARA and MGT. As you know, TMF was part of FITARA's first act. Let's hardwire MGT TMF funding into the FITARA Scorecard. Agencies that score below a C simply are not available to get TMF funds.

The next point is appropriations, appropriations, appropriations. Let's consider the ghost in the hearing room on TMF. When TMF was originally part of the first FITARA package, the draft legislation called for \$3 billion in annual funding. TMF has never been capitalized with more than \$25 million and most years actually has been zero funded.

We need to engage appropriators. Back to Churchill, we will never have a better opportunity to seize appropriators' attention. And, industry, here is an opportunity for you to get involved. Engage through the trade groups to talk to appropriators about this issue.

My fourth point, danger ahead, IT's fallen relief funding. A note of caution. As we look to reinforce an evolved FITARA, we see new warning signs that point to new IT sprawl ahead. CARES and other pandemic relief bills provide welcome funding for IT modernization, but in many cases they cut an end run around the CIO's office and indeed FITARA. America needs the relief, but beware of sprawl and any subversive shadow IT subplots.

Last, the next Federal CIO should come from inside the government IT. While I know that this committee does not pick the next Federal CIO, I would be remiss if I didn't make a plea for the next administration to select a Federal CIO that knows government IT from the start. I would laud Ms. Suzette Kent and Mr. Tony Scott, who acquitted themselves very, very well as Federal CIOs.

However, bringing somebody in from outside government creates a massive learning curve. I already talked about the complexity. We should pick somebody that knows government IT. We have a lot of very qualified candidates.

So, it's a play in five acts: attack complexity; evolve FITARA forward for the future; appropriations, appropriations, appropriations; look out for IT sprawl as we see relief funding coming in, much needed relief funding because we want to make sure it doesn't cut around the CIO's office and FITARA; and we need to choose wisely for our next Federal CIO. Federal IT experience will be a huge plus.

Mr. CONNOLLY. Thank you, Mr. O'Keeffe.

Mr. O'KEEFFE. Thank you.

Mr. CONNOLLY. Thank you very much.

Hana Schank, you're recognized for five minutes.

**STATEMENT OF HANA SCHANK, DIRECTOR OF STRATEGY,
PUBLIC INTEREST TECHNOLOGY, NEW AMERICA**

Ms. SCHANK. Thank you for the opportunity to testify today. My name is Hana Schank, and I am the managing director of the Public Interest Technology Group at New America, a think and action tank, and I've spent over 25 years working in technology in both the public and private sectors.

I want to start with a story.

Lisa Charles lives outside of Charlottesville, Virginia. The 42-year-old divorced mother of two typically qualifies for the Earned Income Tax Credit. She works when she can, but spends the bulk of her time tending to her older son's severe medical problems. His endocrine system does not function properly, and he spends a lot of time in and out of the hospital.

Because Charles was below the filing threshold and had not filed 2018 or 2019 taxes, she was one of an estimated 12 million Americans who had to claim her stimulus check using the IRS's non-filer portal.

In March, sitting beside her son at the hospital, she filled out the form. She really needed the money because she was behind on rent and facing eviction.

To date, she has not received the stimulus money for her children or the \$2,148 she qualifies for under the Earned Income Tax Credit.

What Charles didn't understand is that the non-filer portal prevents its users from claiming the EITC. As a work-around to allow non-filers to claim a stimulus check, the portal files simple tax returns for its users, unbeknownst to Charles and millions of other Americans. So, when she attempted to claim the EITC, because she had used the portal, the IRS said she had already filed taxes and couldn't do so again.

To remedy the situation, Charles must mail a 1040 form to the IRS and wait for the agency to work through its backlog to get to her. In the meantime, Charles' bills won't wait.

When it comes to Federal IT failures, we are used to hearing stories about websites crashing or huge cost overruns and delayed launches. But Charles' story is, more and more, what Federal IT disaster stories will sound like.

Unless the Federal Government changes its approach to technology, badly designed systems—layered on top of a badly thought through process—ending up in a total failure of service delivery for the people who need it most—is our future.

Yes, it is true that the Federal Government often relies on IT systems that date back to the 1950's, which doesn't help matters. But two bigger issues created the Catch-22 that Charles and millions of others are caught in. And it is worth noting that while this example is specific to the IRS and the CARES Act, it could be happening with any agency and any new policy at any time.

The first issue is that these systems were built for a time when people didn't use computers from home. They are built for phone, mail, fax, or in-person contact.

The second issue is that when government implements a policy, that policy implicitly relies on existing IT to be delivered. But the policy creation process doesn't take delivery into account.

Congress is used to enacting policy and having it then be a reality. In today's world, there is an entire technology component that must be put into place in order to make policy a reality.

For something like the CARES Act, that money doesn't exist for the people who need it until they're able to successfully file for and receive it.

This means that policymakers need to think about things like, how will people apply for this? What systems will this rely on, and

what is the status of those systems? How will people track the progress of their applications, just as they can track a package they ordered online? This transparency into government processes is essential.

Thinking about delivering means thinking about all the different types of people who might file for something, thinking about how they might file, and what might go wrong. Businesses would not survive without thinking this through, yet it mostly doesn't happen in Federal IT projects.

So, what's the solution?

First, there needs to be a modern technology work force inside the government, and this starts from the top. There must be a very senior person at each Federal agency who has a background in technology, who can bring that experience to bear on policy decisions.

Second, all policy decisions must include a tested delivery plan. That should start here in Congress.

Finally, I want to touch on cost savings. When IT fails, it is expensive. We see cost overruns into the billions of dollars.

Bringing senior tech talent in-house, while potentially expensive as a line item, would likely lead to tremendous cost savings as there would be people who could advocate for building the right thing the right way the first time. There would be no need to patch unforeseen holes quickly as the IRS was forced to do with the CARES Act. Government would get it right, save money, and serve the people the way it is intended.

Thank you.

Mr. CONNOLLY. Thank you, Ms. Schank. Thank you.

I would note before calling on Ms. Norton, if you look at the FITARA Scorecard, Ms. Schank, you will see that one of the categories of the scoring is the empowerment of the CIO to make decisions at the top and to make sure that person reports to the boss so that we're empowering it and investing it with authority as well as responsibility.

We also as part of FITARA, when we actually wrote the bill, were focused on the last point that you made, about bad projects, or projects that go bad, and being able to pull the plug quickly so that we minimize the fiscal damage. Again, FITARA encourages that and authorizes that.

OK. Ms. Norton, are you with us? Delegate, Congresswoman Eleanor Holmes Norton, are you with us?

Ms. NORTON. Can you hear me now?

Mr. CONNOLLY. Yes, we can. Thank you.

Ms. NORTON. All right.

Mr. CONNOLLY. There you are.

Ms. NORTON. The first thing I want to do is to thank you for this hearing. It is a very important hearing. You and I both represent many Federal employees, so it's of special concern to us both.

I do want to note that I have been concerned with the Federal work force for some time and had a bill in before we attained the majority aimed at recruiting new Federal workers. I was astounded to find out that essentially only 20 percent of Federal IT workers are under the age of 40, which meant that we were just losing out and losing all opportunities.

And, Mr. Chairman, I do want to say that I did get back a thoughtful letter from Director Dale Cabaniss indicating some of the things that the Federal Government has been doing in order to try to help the Federal IT work force enter into the 21st century.

Ms. Schank, this failure, I want to focus on this really abject failure to modernize the IT in the Federal sector, whether that is simply resistance or failure to just keep up.

Ms. Schank?

Ms. SCHANK. The question is, to what degree is the lack of modernization due to resistance versus just lagging behind?

Ms. NORTON. Yes. Yes, active resistance as opposed to inhibitions on the agencies to move ahead.

Ms. SCHANK. I don't think that it is resistance so much as just not having a clear way forward. You know, a lot of agencies have yet to see that without—that their policies are—the policy is reliant upon delivery and that delivery is reliant upon IT systems. So, because that connection hasn't been made, there is sort of a lack of, I think, interest or just understanding the importance of why you would want to bring people in to create a modern tech work force or why that is relevant to the agency's mission.

Ms. NORTON. This a question for any of you.

Mr. O'Keeffe, I'll start with you. Have funds been at the bottom of this? If we were to somehow come forward with an appropriation, would that be enough to get the attention of those in the Federal agencies or is it other kinds of resistance?

Mr. O'KEEFFE. Thank you.

I think funding is definitely a factor, and I talked about the requirement to fund the TMF as part of MGT and bring that together with FITARA.

But I do feel like the biggest challenge overall, I don't think it's an active resistance issue, to your question earlier, it's the complexity of what's going on. It is an acronym soup, and it's a compliance culture.

So, how do we simplify and provide greater transparency in order to move the ball forward? I think those are—

Ms. NORTON. But these workers who have been in the government for a very long time, do you think that we need wholesale retraining? You noted, quoted statistics showing that young people don't even want to come into the IT work force of the Federal Government. Is that the problem or is it a retraining problem?

Mr. O'KEEFFE. I think it's a problem on multiple fronts. So, yes, absolutely training is very important.

I don't know that the Federal Government of late has been a particularly attractive employer for young people. Now, with the pandemic and the downturn in the economy, we'll probably see government jobs being more interesting.

Ms. NORTON. I must say that this would prove the notion, and they do say, OPM, that they do recruit. I think there is a major issue of how you make the Federal Government jazzy enough so that these young IT professionals want to come in.

Mr. Cornelius—

Mr. CONNOLLY. I'm afraid the gentlelady's time has expired.

Ms. NORTON. Thank you very much, Mr. Chairman.

Mr. CONNOLLY. Thank you, Ms. Norton.

Mr. Hice, you're recognized for five minutes.

Mr. HICE. Thank you, Mr. Chairman.

Mr. Cornelius, as I understand it, one of the reasons Federal agencies do not readily purchase commercial off-the-shelf items is because there's no incentive to prioritize those type of technologies over developed in-house type things. So, from that mentality, what kind of policy solutions do you think ought to be proposed in order to remedy that problem?

Mr. CORNELIUS. Thank you, Congressman.

So, there's a couple of things there, and I think both Congresswoman Norton's question and yours sort of dovetail together. So, part of it is incentives and part of it is an understanding.

So, the work force that we should care about inside government is not just the IT work force when it comes to modernization. Everyone is an IT worker in government. Everyone uses and leverages technology to deliver the programs, the products, the services they're there to deliver.

Therefore, we've got to make sure everyone has a relevant understanding of what's happening in the technology market so that when we actually do go out and try to procure the vast majority of the technology that is used in government, that the procurement executive, the technology executive, the finance executive, the H.R. executive, they all understand why the technology is important to them.

So, understanding and creating a better sort of policy and understanding around how fast and how up to date the technology market is driving, that will create a better understanding so that when agencies are trying to either retire old bespoke systems or simply just acquire and use newly technologies to pilot them or to try and scale them in government, that they actually understand what is happening in industry so that they can leverage it more effectively.

Mr. HICE. OK.

Well, let me, Mr. Bitko, let me go to you right along this same train of thought here. During your time as the CIO with the FBI, what were some of your experiences trying to procure commercial IT solutions? And along those lines, to what extent were there incentives to purchase commercial?

Mr. BITKO. Congressman, thank you for the question.

There definitely are incentives for the IT individuals to procure commercial products. But as Mr. Cornelius said, the issue I think is that everybody is an IT worker, and the mission users of those systems, they know what they want. What they frequently want is not the commercial product but something that has been customized in some way. And the results when that happens is you take a lot of time taking the commercial products and customizing it into something that then becomes a legacy product that is difficult to maintain and support.

I have a quick example that highlights that. For the FBI, the time and attendance system, you would think that that is a standard commercial product, right, that everybody tracks time and attendance in the government and wants to know how long everybody works.

Well, the FBI had customized the time and attendance process over the years for a variety of reasons, some of them reporting to

Congress or for internal management, but to the degree that the commercial product was no longer in sync with the customized version that the FBI was using.

The result of that, unfortunately, is that every time the vendor updated the commercial product, it was many months of work, sometimes years of work to figure out how to backfit those upgrades to the version that the FBI was using in ways that would prevent it from catastrophically failing.

So, the crazy thing out of all of that is that the FBI time and attendance system still runs on a restricted network that is not accessible when you're out of the office. So, if you wanted to record time and attendance, you have to physically be in an FBI location to do that.

So, the disconnect, sir, is between the incentive to leverage and to buy commercial products and all of the business users, the mission users, who have their own needs, and figuring out how you balance the costs and benefits between changing the internal process so that you can use the standard product versus adopting it in order to meet some unique need or mission.

Mr. HICE. Sounds like we are masters at complicating the issue is the bottom line, and it doesn't need to be that way.

Mr. Cornelius, I want to come back to you with this, but I would ask all of our witnesses if you could respond in writing to this question because I would be interested in hearing from all of you.

But what changes would you make to the structure and process for awarding project funds from the TMF?

Mr. CORNELIUS. So, there's a couple of things. Given the current amount of appropriations, which is somewhere short of \$150 million, which is all it's gotten over the last three years, the best we can do is make small-bore project delivery decisions.

So, the board has, from my time at OMB, we had more than 50 projects that were submitted, costing, I think, more than about \$600 million, and we only had \$150 million with which to try and dole out to that. In doing that, you can only support sort of agency-specific projects.

I think the model needs to be flipped on its headfirst. I think Congress, including former Ranking Member Meadows, who was a big fan of the TMF, now the current Chief of Staff, should be pushing to make sure there's a billion dollars in TMF funding in the next phase 4 bill.

Then OMB and GSA should be looking across the Federal enterprise to figure out where those investments should best be, whether it's an individual agency or hopefully in multi-agency programs and process improvements and digital capabilities that agencies are learning about right now in the midst of the pandemic.

So, I think if they had more money, plus if they allowed for both individual agency projects while also sort of looking across the Federal enterprise to make enterprise investments, that could lead to tremendous benefits, both now to fight COVID-19, as well as well into the future, and retire some of these legacies.

Mr. CONNOLLY. Would my friend allow me to just add to the point you're making?

Mr. HICE. Yes.

Mr. CONNOLLY. Just real briefly.

So, you called for a billion dollars in the TMF, the Technology Management Fund, which is, in fact, provided in the HEROES Act pending Senate action. I think you would agree, and I think my friend would also agree, that \$25 million, as appropriated in the last appropriation, is simply meaningless.

Mr. CORNELIUS. Yes, Congressman, it is wildly inappropriate. I spent the past several years in OMB working through the budget process and working with appropriators not to just talk about the value of the TMF, but to also find ways to do it.

And, frankly, outside of an emergency situation like this where Congress can go above and beyond the sort of 302(b) allocations that they have on the normal Fiscal Year sort of appropriations cycle, you're never going to get that amount of investment that is necessary so that OMB and GSA and agencies can really start to transform the government.

Mr. CONNOLLY. Thank you.

I took some of my friend's time. If you wish—

Mr. HICE. No. Thank you, Mr. Chairman.

Just by way of reminder, I would like to hear from the other witnesses on this to get their answers as well.

Mr. CONNOLLY. Certainly.

Mr. HICE. Thank you. And I yield back.

Mr. CONNOLLY. Certainly. Thank you.

Ms. Schank or Mr. O'Keeffe, do you wish to comment?

Mr. O'Keeffe?

Mr. O'KEEFFE. Yes, I think that the gentleman covered it down very well. I think that the last time I testified on IT modernization, GAO told us there were 777 supply chain systems and 622 H.R. systems in the Federal Government. That was 10 years ago. I would guess there are probably more than that. So, it's this ability to build that Mr. Bitko talked about which I think is the real enemy, customization.

Mr. CONNOLLY. Thank you.

Ms. Schank, did you wish to comment?

Ms. SCHANK. Yes.

So, the customization piece versus buying, so I think we are working with a slightly outdated view of how tech gets built. It used to be that people would buy something and do a lot of customization. The example would be the FBI system. That sounds to me like that was a really old system that was customized and updated repeatedly. I mean, I'm guessing, but that sounds like a decades-old system.

I think that modern technology is a lot more flexible. And, of course, there will always be some degree of customization. But no technologist would ever start a project without first thinking about what exists on the marketplace. That is just that's how you do it. Nobody is sitting there thinking, "Oh, boy, I want to build something from scratch because it's fun." People will definitely look into what's out there first.

Mr. CONNOLLY. Thank you.

I will say this. The FBI example is one I actually happen to know about wearing a different hat, and I can tell you that part of the problem was FBI. They kept on changing the scope of work. They kept on adding to it. They didn't have experts who understood the

limits as well as expansive potential of technology. As a result, they absolutely designed something that could not work and would never work, because they really didn't understand how to create the terms of reference for a real contract that could provide a real product that worked.

So, part of that problem is internal expertise in our Federal agencies in even understanding the scope of their own needs. And having translation between the highly technical and the operative at the layman's level is a real challenge for the Federal Government, especially, as Ms. Norton pointed out, as our work force ages and is less technologically savvy than the generations succeeding us, that gap grows.

Anyway, let me see.

Mr. Lynch, are you with us? Steve Lynch?

Mr. Lynch?

Is Mr. Massie coming back, Mr. Hice?

Mr. HICE. I don't know.

Mr. CONNOLLY. OK. Mr. Grothman, is he coming back?

Mr. COMER. I don't know.

Mr. CONNOLLY. Ms. Plaskett, are you with us?

Ms. PLASKETT. Yes, I am.

Mr. CONNOLLY. Great. You're recognized for five minutes.

Ms. PLASKETT. Thank you very much, Mr. Chairman.

And thank you to all of the witnesses who are testifying today.

I have just a comment and then a couple of questions quickly.

On March 16, the Office of Personnel Management directed agencies to maximize use of telework in response to the coronavirus pandemic. Telework proved critical to ensuring the continuance of government operations during the pandemic. Nonetheless, the rapid shift to remote working exposed agencies to increased cybersecurity threats.

So, prior to the coronavirus pandemic, the FBI received about 1,000 cybersecurity complaints a day. That number has since jumped to between 3,000 and 4,000 complaints per day.

The Pandemic Response Accountability Committee reported that since the pandemic hit inspectors general have reported increased risk of data security breaches, disclosures of classified information, and targeted cyber-attacks and fraud schemes.

So, I wanted to ask, Ms. Schank, how has outdated Federal IT exposed agencies to unique cybersecurity threats during the pandemic?

Ms. SCHANK. So, I will preface this by saying I am not a cybersecurity expert. However, a combination of people working remotely and legacy IT, it does not surprise me that there have been—that cybersecurity has been an issue. And it's really not my area, so I'll stop.

Ms. PLASKETT. OK. Do any of the witnesses have any comments or questions on how the outdated IT exposes agencies during this time to cybersecurity threats?

If not, Mr. Bitko, before joining ITI you served as the chief information officer at the FBI. At a high level, what cybersecurity vulnerabilities in Federal IT systems did you detect?

Mr. BITKO. Congresswoman, thank you for the question, and I will wrap in a response to your prior question as well.

Ms. PLASKETT. Awesome.

Mr. BITKO. Because there's an obvious connection here between them. And I'm also going to caveat that by saying, as the CIO my responsibilities were not in the FBI's cyber mission but in the management of the FBI's own internal IT resources.

Nevertheless, just the nature of the organization and being an executive within the agency, there are certainly numerous opportunities to be exposed and work closely with our cyber investigative programs while I was at the FBI.

The range of cyber incidents that are detected are too many to count. There are adversaries out there who will seek any opportunity that they can to take advantage of weaknesses in systems.

Legacy systems are a very core part of that. You can look at both internally, within the Federal Government—the OPM breach is a really good example of legacy systems that were vulnerable because, since they were so dated, monitoring them is very difficult and wasn't done at the level that it should be.

And you can translate that to a lot of the vulnerabilities that the FBI saw at state or local governments that were subjected to ransomware attacks. Again, many of those ransomware attacks were not because there weren't solutions to mitigate against those things, but because those locations, those localities were still running old, outdated systems. They hadn't patched. They hadn't made investments in cyber resources. And the result is, is that they were compromised.

Mr. BITKO. I think, when you translate that to now, to the pandemic, it's exactly the same, just magnified. It's an opportunity for adversaries who are seeing a more distributed work force, leveraging all sorts of their own personal technologies in other ways to connect back to Federal information technology systems, and that presents an opportunity. The need to telework is clear. There's no doubt. But a lot of the security systems, the operation centers that are designed to monitor and collect all this data, they weren't built with the idea in mind that the work force is going to be 20-or 30-or 100,000 agency users working from their home on a home computer and telecommuting in over a VPN or over a virtual desktop.

So, I think that there is a real vulnerability there in that we as the public sector are just not monitoring at anywhere near the same degree that we should. So, that's an additional complicating factor that makes the risk high.

Mr. CONNOLLY. Ms. Plaskett, I wonder if you would have Mr. Cornelius respond to that as well, if that's all right.

Ms. PLASKETT. Oh, sure. Uh-huh.

Mr. CORNELIUS. Thank you, Chairman.

And thank you, Congresswoman.

I think what has come out of the COVID response and the sort of maximum telework posture is that agencies that were already expanding the use of telework within their agencies already had a work force that was trained and capable of using these commercial technologies or these distributed technologies, like Mr. Bitko said, working through VPNs, virtual desktops, et cetera. So, agencies that had digitized the workflows and not just tried to digitize their work force were able to actually make this happen more effectively.

So, I think I believe the practice, as well as GAO in their detailed response to the initial steps to deal with the COVID response, both highlighted that agencies that were already working to expand telework had a trained work force that knew how to do this so that they perhaps were able to better understand and spot phishing attempts that were trying to come through networks or trying to get them to click on suspicious links or were more capable of not having to make workarounds in order to meet their mission responsibilities and can instead work through the agency protocols and processes to do this securely and effectively.

Thank you.

Mr. CONNOLLY. I thank you.

And I thank you, Ms. Plaskett.

Ms. PLASKETT. Thank, Mr. Chairman.

Mr. CONNOLLY. What's that?

Ms. PLASKETT. Yes, Mr. Chairman, thank you so much for time, and I'm just hoping that at some point the witnesses can give us not only best practices but how should Congress structure funding to help the government best modernize IT and meet these challenges. But thank you for this great hearing where we can discuss these issues.

Mr. CONNOLLY. You know, you make a very great point, Congresswoman Plaskett.

And I would just say I would hope that, as part of the post-pandemic assessment, we look at what did not work well and what did work well within the IT context, to your point, because if we don't take away the relevant lessons, we're going to repeat the mistakes.

I have heard some success stories, as well as failures. So, I think you're absolutely onto that, and I'd be glad to work with you in perhaps talking to GAO to get ready for of that kind of analysis.

And I assume, Mr. Hice, you'd join us in a bipartisan way with respect to that. So, thank you.

Glenn Grothman, you're recognized for five minutes.

Mr. GROTHMAN. Thank you. First of all, I'd like to make a suggestion. I always love this hearing.

Mr. CONNOLLY. Certainly.

Mr. GROTHMAN. But there was a little disagreement at the beginning about the mask policy, and I think as long as I've been alive I've never been around a topic on which the experts so consistently get things wrong. I keep getting emails from different constituents saying, "Why do I have to wear a mask?" And while it's true you find experts who think it's good, we're wearing a mask, there are experts who are out there who think we shouldn't be wearing a mask. So, I'm going to suggest that we have a subcommittee hearing on masks, and it's certainly a hot topic back home. Nobody back home asks me about IT in the government, but they all ask about masks. So, it would be good for ratings.

Mr. CONNOLLY. You intrigue me, I would say to my friend, because you could put it in the broader context of, you know, experts.

Mr. GROTHMAN. Right. Experts on both sides.

Mr. CONNOLLY. Right. Right. And that might be a worthy hearing. So, we'll file that away. Thank you.

Mr. GROTHMAN. Good. Now—

Mr. CONNOLLY. Now, Mr. Grothman.

Mr. GROTHMAN. Back to the topic at hand, this will be either for Mr. Cornelius or Mr. Bitko.

The Technology Management Fund was intended to provide agencies with access to funding that was not bound by the annual appropriation process. Can you describe why funding IT modernization projects should not be bound by single-year increments?

Mr. CORNELIUS. Thank you, Congressman. It's a great question.

So, most of the times we talk about retiring a legacy system, it means it's a system that's been built over years and years and years with subsequent years of funding and sort of more technology or products sort of glommed on top of it, which means, if there is an agency plan to retire that system, the likelihood is that it's going take multiyear funding. It's going take funding over multiple years to retire it. The system cannot just shut off automatically. So, you're going to need consistent funding in the outyears to do that.

As we know, there's oftentimes disagreements between the executive branch and the legislative branch on sort of funding levels and things like that. So, agencies are often at the whim of appropriators and the appropriations process to do that. So, that's why an investment in the Technology Modernization Fund, those are no-year dollars, and the money is flexible so if that a project is going well, money—more money can be provided to help accelerate that modernization process and move it through more quickly. And if it is going poorly, the TMF board can help course correct or, you know, help that agency remediate some problems or discontinue the project all together so that it's not a project where the agency is committed to years and years and years of a contract when they already know the project is failing.

Mr. GROTHMAN. OK. Thanks.

I'll give you a kind of a followup question and if Ms. Schank wants to weigh in, too.

As more Americans continue to interact with the Federal Government to understand benefits and receive critical information, understanding the customer IT experience will be critical. What challenges do agencies face when trying to improve the design aspects of their systems?

Mr. CORNELIUS. I'm happy to let Ms. Schank go first, or I can start. Her call.

Mr. GROTHMAN. She can go. It's her turn. We'll give her a shot.

Mr. CONNOLLY. Ms. Schank?

Ms. SCHANK. Thank you.

One of the huge barriers for agencies as they try to bring in customer experience into their systems is that there is a lack of feedback loops that are currently in place. So, traditionally, when you look to incorporate user research, you have a—there's an easy methodology. There's an easy way to do that, but a lot of agencies aren't collecting user feedback on specific pieces of how a certain agency is fulfilling its mission and in a meaningful way that then plugs into the design of the system.

Did that—does that make sense?

Mr. GROTHMAN. Yes.

Do you want to followup, Mr. Cornelius?

Mr. CORNELIUS. Yes, Congressman, I think, again, it goes back to that issue I raised in my opening statement about the legacy

being a cultural problem, is the dollars that any Federal agency's using to spend on technology supports a system and a program that is there to serve the public. So, the first issue before any agency thinks about a technology system or a program is sort of, how is the execution of that program and the underlying technology that makes it happen, how do we know that's going to benefit the citizens whose taxpayer dollars are the ones funding it?

So, I think if agencies can start with citizens are not just there to allow the government to execute on a mission but the citizens are the recipients of that mission and they should be provided those benefits and those services effectively, the same way they get on their iPhone or, you know, with package delivery or anything else. So, I think that mindset of putting the citizen, putting the customers first would help sort of alleviate some of these bottlenecks we get where agencies are just designing systems for themselves and not for the end user.

Mr. GROTHMAN. Thank you.

Mr. CONNOLLY. Thank you, Mr. Grothman.

Mr. Raskin, you are recognized for five minutes.

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

A quick point on the subcommittee health protocols. You know, if there are Members, as the ranking member suggested, and I have no reason to doubt him, but if there are members who are not coming in because they so resent the rule that we've adopted based on the Capitol Physician's advice, there are also Members like me who are here who are in Washington, who are at the Capitol, and I'm in my office because—simply because I just I can't subject people in my family to the risk of having Members not wearing masks for whatever reason they might have.

I also think we should not be party to confusion and disinformation about masks. I'm not seeing any dispute at all from the expert medical authorities that we follow. The Centers for Disease Control is recommending cloth masks for everybody who is in public, in public spaces, and as well as social distancing. The World Health Organization is recommending masks. In fact, if you look in the countries that have actually brought the virus under control like in Europe, the masks have been central. And it has been the President's dereliction of duty in sending all kinds of mixed messages about masks that has made us now No. 1 in case count and No. 1 in death count around the world. So, there's really no confusion about this. And we should not be spreading confusion.

Now, Mr. Chairman, as to the matter at hand, obsolete IT systems have created a lot of headaches for our constituents seeking unemployment benefits and stimulus checks. At our hearing last month, we found that our government didn't shut down during the pandemic. It ramped up to deliver new and existing services amid these extraordinary challenges. At many agencies that had modernized before, Federal workers could continue operations and serve constituents effectively because their updated systems allowed for remote work; not so for a lot of other agencies.

We've been arguing for decades in the subcommittee that telework is important, and now the pandemic has finally forced government administrators to take remote work seriously. Some were ready, and others were not. We know that GSA was the Fed-

eral Government's biggest adopter of telework and that made it well-equipped to continue its work during the pandemic, but many agencies failed to invest in IT and deferred digitizing. And now they're calling back employees, putting the health and safety of these workers in danger because their leaders had failed to prioritize IT.

The IRS asked staff to return to perform tasks that could be digitized, automated, or performed remotely like answering phones or processing mail.

Mr. O'Keeffe, your company conducted interviews with many of the CIOs on their experience in modernizing IT and transitioning to telework in the pandemic. What were some of the lessons learned and best practices that emerged from this study?

Mr. O'KEEFFE. So, the CIO has across the board lauded telework. I think it's going to be very difficult to put the genie back in the bottle on telework. And I think, as Mr. Cornelius mentioned earlier, the idea of practicing telework before the pandemic struck, those agencies that had practiced and had systems in place were a lot more successful and those that went forward in terms of cloud computing also found their ability to telework and to be more agile, to be more customer-centric significantly enhanced.

Mr. RASKIN. Thank you.

We also have to work with technology out in the field. There are those who inspect mine safety, who inspect poultry, who audit agency operations. And these employees rely on tech as well.

Mr. Bitko, when you were at FBI as the CIO, you had to manage a lot of agencies out in the field. How would you make sure today that your work force could continue operations during a global pandemic?

Mr. BITKO. Thank you for the question, Congressman.

There's no doubt that telework is essential to enabling that. It really comes back to, again, the point that Mr. Cornelius was making that the agency needs to be planning for this sort of environment and building technology that enables in the case of the FBI's agents who are sitting out there in the field to do their work. One of our goals was to go even beyond that, not just in the field offices, because they all have good connections, of course, but agents, their livelihood is out in the world, talking to people.

Mr. RASKIN. Yes.

Mr. BITKO. The more technology we can give them actually to be effective while they're doing, the more effective they can be. So, I think it's the agency cultural change to that mindset of using technology.

Mr. RASKIN. Ms. Schank, how can the Federal Government do a better job ensuring continuity of operations during moments of national crisis that require rapid response?

Ms. SCHANK. COVID and what we will potentially see again is what happens after decades of neglect and what that—what that looks like to us is that the technology is outdated. But if you dig into why the technology is outdated, what you come up with is that the Federal Government is short on internal technology teams and long on massive vendor contracts so—which is not say that building an internal agency team means an end to vendor contracts, but an internal agency team is certainly something that would be a lot

more flexible and able to build a modern—build a modern tech stack.

Mr. RASKIN. Thank you very much, Mr. Chair.

I yield back.

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

Mr. Norman, you're recognized for five minutes.

Mr. NORMAN. Mr. Cornelius, you mentioned in your opening statement technical debt. You said it leads to wasteful spending and outdated IT. Can you define exactly what that is?

Mr. CORNELIUS. Yes, I think the easiest definition is technical debt is the continuance of old and outdated technology inside agencies or that agencies are reliant upon that is not modern and sort of updated to commercial best practices. So, agencies being reliant on old processes and old software or old systems to do things where modern commercial sort of analogous practices and capabilities are already available and are already widely adopted by citizens and companies.

Mr. NORMAN. It could be a generational thing, too, couldn't it?

Mr. CORNELIUS. I do think that a lot of the old technology—again, there's something that I always bring up is everything is abnormal until it's normal, and I think COVID is a tremendous sort of example of that. I mean, no one would have been in here, wearing mask, and sitting this far apart in a normal hearing. And I think that's the same thing for agencies. So, I think, to the chairman's point, there's going to be so many agencies and people with inside agencies that are going realize that they could have already done so much more and were so capable already because of the response that they've done due to distributed telework and the CARES Act and everything else.

So, again, it's not just generational, but it's also sort of habitual. It's people are comfortable what they're comfortable with, and they'll use old, clunky systems if that's all they know how to do, rather than try pick up and sort of leverage the newest sort of whizbang technology.

Mr. CONNOLLY. Would my friend yield just for a second?

Mr. NORMAN. Yes, sir.

Mr. CONNOLLY. Because I think you're making a really good point. It's also the cost.

Mr. CORNELIUS. Yes.

Mr. CONNOLLY. The cost of retiring a legacy system can be in the billions of dollars and take multiple years, and you've got to retrain everybody, and it's just easier sometimes to decide, "Let's put that off this year," and that keeps on going. And I think that's a real factor in management's decision to defer these kinds of things, and suddenly they wake up and realize they're 30 years late.

I thank you for yielding.

Mr. NORMAN. Yes, sir, Mr. Chairman.

You know, and I agree because, you know, I don't know how you get—I don't know how you get that, particularly with the older generation, how you get that sunk into their heads that this pays off. It's keeping up with the times. And if you don't do that, then you're jeopardizing the whole system.

Mr. Cornelius, this is for you, too. The GAO found that Federal—many of the Federal IT investments have suffered from a lack of

effective project management. In the private sector you can take care of that. If you get ineffective project management, you deal with it. Either you make it effective or you get rid of that person or groups so that it's effective.

How is—what's your opinion on the best way to tackle this and to get the problem solved and find from your, from where you sit, what your opinion of that statement is?

Mr. CORNELIUS. Thank you, Congressman. So, I think it's a multifaceted answer, and I won't try to talk too long because I know you probably have some more questions but it's a couple of things.

One, the work force needs to be well-trained and well-equipped to know how to actually manage projects effectively. Project management, just like IT, just like finance, just like HR, acquisition, they're not just the other person's job that you work with that are in an office. They're part of how you go about sort of managing your day-to-day and how you go about executing your mission.

A lot of the—another thing I found when I was in government is a lot of the project management, as I think you defined it in the private sector, is outsourced to a lot of these vendors who will come in and say that, you know, I will build what you whatever you want built, and then I will manage it however long you want me to manage it and update it. And you, all you have to do is make sure that we're hitting some certain milestones or metrics that you put out there.

That is certainly a way of doing business, but I don't think that is the most effective—I don't think anything anyone in the private sector would do it that way, and I think Ms. Schank has referenced the fact that folks like the U.S. Digital Service and others have come in with that mindset and provided some good examples and opportunities for agencies to change. And they're not there to change it for them but they're there to show them there's a different way to leverage technology and to be more effective and to manage projects, to get lower costs and better outcomes.

I think to the extent we can continue to proliferate and help all of the Federal work force understand that and be trained effectively would lead to a lot better outcomes in both the use and management of technology.

Mr. NORMAN. And the bottom line is results. You get results, and it dovetails in with the technical debt that you were talking about.

Mr. CORNELIUS. Absolutely. Like I said when Mr. Grothman was asking his questions, we have to treat the American taxpayers like customers because that's what they are. They are reliant on government benefits and services, but they should also be treated as recipients and as people that agencies are there to serve and agencies aren't just there to sort of manage their own operations as they see fit.

Mr. NORMAN. Thank you.

I think I'm out of time. I yield back.

Mr. CONNOLLY. I thank you. I thank you, Mr. Norman.

The gentleman from California, Mr. Khanna, is recognized for five minutes.

Mr. KHANNA. Thank you, Mr. Chairman, and thank you for your continued leadership.

I have a bill H.R. 5901, which Matt Lira helped us with and with Senator Portman to codify the Centers of Excellence at GSA. We've heard testimony they'll provide services to agencies to improve Federal IT across the executive branch.

Mr. Cornelius, what role do you see these Centers of Excellence playing in help speeding up IT modernization throughout the Federal Government?

Mr. CORNELIUS. Thank you, Congressman, and thanks for the call out to Mr. Lira. I had a great time working with him when I was at the Office of Management and Budget and he was at the White House.

I think, to the extent that we can make it open and able for new ideas and new technical talent to come into the government to help either individual agencies internally or agencies sort of across the enterprise buy and use commercial technology to achieve mission outcomes, I think that should be celebrated. I think there have been conversations in Congress over the years on whether to codify things like the U.S. Digital Service or 18F or now the COEs, and while I think those are steps in a direction, I also think it's a little bit like having your cake before eating your broccoli with your meal. I think you need to focus on getting the entire work force up to speed and elevating the skills of all the people that are going around and are constantly managing these programs. And then we can think about the best way to sort of collect and manage and oversee and appropriate any of these digital services teams or other new types of business models inside government to drive better outcomes.

Mr. KHANNA. Thank you.

Do any of the other panelists want to speak to that or about the oversight role that Congress should play on Centers of Excellence?

Mr. BITKO. Congressman, if I could add an additional point to that, I think that one of the big challenges with Centers of Excellence or centralized services being provided is the FISMA challenges around reciprocity between different agencies. And if an agency, if one agency delivers a service or a Center of Excellence delivers a service, as long as FISMA is making it the responsibility of another agency's CIO or another agency's senior leadership to accept risks, they're unlikely to feel comfortable just accepting the work of the Center of Excellence. They're going to end up redoing a lot of it themselves.

I think that is significant friction in the system for the idea of centralized service services being provided, and that is something that needs to be looked at.

Mr. KHANNA. What would you recommend as a solution to that?

Mr. BITKO. I think, sir, FISMA has to be really modernized. I know that has been touched on here a little bit. FISMA is important, no doubt. Information security is essential to all the work that's being done, but, much like we're talking about modernizing legacy systems, security practices have to be modernized as well. And today there is still—there is a lot that's done in the individual agency interpretations of NIST, and the individual CIOs get to make decisions about what levels they're going to accept and how they're going to do it. I think there has to be some work put into thinking about how to do that and to provide for some consistency

in interpretation of the NIST standards and FISMA across the board. Otherwise, again, we're going to still have these conflicts.

Mr. KHANNA. Do you or any of the panelists have a view how our Federal agencies when it comes to technology proficiency, technology use compared to the rest of the world? Are we one of the world's leaders? Are we lagging?

Mr. O'KEEFE. If I might go back to the question about COEs, one point I would raise—

Mr. KHANNA. Sure.

Mr. O'KEEFE. One point I would raise is it's inconsistent. So, the agencies that have been through the COE process, one would anticipate that they would do better on the FITARA scorecard than the agencies that have not been through the COE process. That does not seem to be the way that it plays out. So, there's kind of a head scratch on the COEs. Again, how do we simplify, and how do we understand how agencies are actually performing?

Mr. KHANNA. If you have ideas on how we can strengthen it as we work through this bill, we'd obviously welcome that.

Mr. O'KEEFE. Yes, I think on the work force issue, I think it's in pockets, but there's definitely a requirement for training at scale in the Federal Government. So, when we talk about the Cyber Corps and such initiatives, we're talking about 10's, 20's, 50's. We need to be talking about thousands. So, how do we create scale for IT work force training in the Federal Government? That's really the big question.

Mr. KHANNA. Very good point.

Let me ask one final question. The—I passed last Congress the IDEA Act. The President had signed it, 21st Century Integrated Digital Experience Act. How would we benefit from agencies fully implementing the IDEA Act, and do we have any sense of whether it's working or not?

Mr. CORNELIUS. May I, Congressman?

Mr. KHANNA. Please.

Mr. CORNELIUS. So, first off, thank you for your leadership on the IDEA Act. I think it's an incredibly important piece of legislation. And it goes back to some of the questions we've had from both the majority and the minority on sort of how we make digital services' information websites more accessible, usable, and easier to understand for the public.

And I think Ms. Schanks' opening statement, when she told that very heart-wrenching story of the lady who could not actually apply for benefits, is one—is a case in point for why something like the IDEA Act is important. And, frankly, I would request that my former colleagues at OMB hurry up and get the IDEA Act guidance out there. I think there's a lot of agencies that might still be waiting on the Office of Management and Budget to really help push them in the right direction and point them to where they should go, and I think that bill gave OMB a lot of deference when it came to guidance on the IDEA Act.

But I will say from at least an industry perspective, you know, no company that is worth its salt would be up and running if it was not able to easily and effectively convey what its mission is and what its services are to potential customers. And so, I think I agree with you that we should continue leveraging the IDEA Act.

And, frankly, I think that's one of the recommendations that my organization has made to Congressman Connolly and his staff on sort of a modernization of the FITARA scorecard.

Mr. CONNOLLY. Thank you.

And I thank you, Mr. Khanna.

We will continue working with you on the modernization. It's not frozen in stone. We just want to make sure we get the basics right before we start branching out.

The gentleman from Kentucky, Mr. Comer, is recognized for five minutes. And congratulations on your selection as our new full committee ranking member. We welcome you.

Mr. COMER. Thank you very much. I appreciate that. Look forward to working with you in the future.

Mr. Cornelius, the Modernizing Government Technology Act and associated Technology Modernization Fund have been important steps forward, but the tasks of modernizing Federal IT systems is truly massive. It's my understanding that these take a very long time, are extremely complicated, and certainly cost a lot of money. They're similar to infrastructure projects like roads and bridges. Should we look at them in a similar manner as infrastructure projects, that is, multiyear appropriations?

Mr. CORNELIUS. Absolutely. And Chairman Connolly actually took my compliment away from me. I was going to congratulate you on also becoming the ranking member—

Mr. COMER. Thank you.

Mr. CORNELIUS [continuing]. To the full committee, but I'm sure there's plenty of compliments to go around.

Absolutely is the simple answer to your question. Most of the money, so not all costs that go into the \$90-plus billion in Federal IT every year is the same about. About 75-, 76 billion of that is just keeping the lights on. It's all this O&M dollars, just keeping the systems afloat. And there's very little there for development, modernization, and enhancement.

So, I do think, while the Technology Modernization Fund is incredibly effective and what has happened on FITARA has been impactful when it comes to elevating the CIO and giving them authority, if most of the money is appropriated to individual programs or individual offices within agencies and they come up with their own decisions and it's just a sort of thumbs up, thumbs down from a CIO, it's very hard for them to really look at things across the enterprise and look at things from a multiyear perspective.

So, to the extent that we can right size Federal IT spending within agencies and make those moneys perhaps multiyear or several-year dollars, I think there's a trade agencies would make in getting more flexibility for the money and allowing Congress and OMB to have stronger oversight of that spending.

Mr. COMER. So, if we're going to require agencies to reimburse the TMF, what's the more realistic timeframe than three years on the reimbursement?

Mr. CORNELIUS. Well, I think on the reimbursement, so especially as part of the \$1 million that I think Mr. Bitko and I have both joined a letter in supporting, I think repayment when it comes to COVID-related issues perhaps should be looked at as sort of being done away with. If agencies are really trying to move fast to

deal with COVID and they have got to leverage the team to have to do it and if Congress doesn't give more money for individual agencies, as they did in the CARES Act, then let's think about ways for projects that are relevant to COVID-19 to make that happen.

But I think, broadly speaking, a lot of the agencies, at least the projects that were funded during my time at OMB, most of those were already well on their way to success, well on their way to repayment. So, I think the model works, but we're also operating in a very different timeframe, in a very different environment, especially in the middle of COVID.

So, I do think there are changes both Congress should be looking at, as well as OMB and GSA should be looking at, to improve the way that fund is leveraged and the impact that it provides.

Mr. COMER. Finally, how good a job are we doing at measuring what the associated savings from these projects are?

Mr. CORNELIUS. It's a very difficult question, Congressman.

Mr. COMER. Right. So, not a very good job.

Mr. CORNELIUS. I would—I would think that—I would think that there's a place, if you're looking at agency legacy modernization plans—and I think GAO talked about that in their report—it's not just the plan that's important. It's the agency budget request that goes into that plan. It's the actual appropriations provided to that plan, and then it's the outcomes and then performance. So, it's not just enough to have a plan. You have to know if there's enough resources coming in. You have to know if the resources that Congress provides meet that need, and even if not, how are you using the moneys that are provided to actually get performance and outcome?

So, I think that virtuous cycle between having a plan and being able to fund it, resource it, and acquire commercial technology effectively to retire old systems and move to new technologies, I think that that's something that where there can be a lot of power in both savings and in performance, which I think are two sides of the same coin.

Mr. CONNOLLY. Would my friend yield?

Mr. COMER. Please. Go ahead.

Mr. CONNOLLY. Because I'd like to just add on to that. I mean, I think there are two things here based on my own experience of 20 years in the private sector. One is you can't have erratic budgets. Right? So, if you do get an agency head who says I'm going to make this a priority and then that agency head discovers in the next budget cycle his budget's been cut 30 percent, all of a sudden that priority collapses.

Second, though, we need agency heads to show leadership. It's not that different. It is different. But in the private sector if a CEO says, "We're going to replace our entire legacy system and you've got two years, Mr. Cornelius, so get it done, and if you don't, I'll find Mr. Comer; he'll do it," guess what happens? Resources get marshaled, you know, because people follow the directive of the management and management has to pay attention to it and make sure it is being done. So, it's not only money. It's also about management will and leadership, if we're ever going to get some of these legacy systems retired.

I thank you for yielding.

If you wanted to comment, Mr. Cornelius, feel free.

Mr. CORNELIUS. Both Chairman Connolly and Ranking Member Comer, that is incredibly well said. It takes—and I mentioned this, I think, in my full written statement, not my opening remarks, which is it actually takes a commitment from leadership, agile acquisition authorities, multiyear funding, strong oversight, and a commitment from the work force to get this done.

So, I think when you have those five pillars all together and you can look at things over a long period of time, not decades but hopefully, you know, a few years to move the ball forward, I think that's incredibly effective, and I want to commend a lot of the CIOs and even agency heads in this administration and in the previous administration who really understood that technology was the fundamental underpinning of how their agency functions and how it delivers services and really made IT a priority.

So, we have a lot of great leadership in the executive branch and in Congress on that point.

Mr. CONNOLLY. I thank you.

And I thank you, Mr. Comer, for yielding.

Mr. LYNCH, I understand that you're back with us.

Mr. LYNCH. Hello, Mr. Chairman, yes, I am.

Mr. CONNOLLY. Good. You're recognized for five minutes. Welcome.

Mr. LYNCH. Thank you, Mr. Chairman.

And, you know, for the 20 years I've been in Congress, I can echo the chairman's concerns as well. We've been dealing with this issue consistently year to year, year in and year out. If there's any one area that shows how slow our government responds to reality and technological change, it's this issue. And we're at a point where we not only need to catch up to and renovate some of the legacy systems, but even some of our systems that have been able to maintain some level of competency are being outpaced now.

I speak specifically to the blockchain network. So, there are a number of applications I think of blockchain that could help us enormously. I have a bill right now that was offered several months ago to put the biodefense stockpile on blockchain so it will be transparent, not an open blockchain but a closed blockchain, a private blockchain with government and some of our state partners.

But I would just offer to any of our witnesses. Do we have the ability to try to leapfrog some of these legacy systems by adopting the blockchain, you know, a blockchain type system to replace some of the old, you know, bureaucratic, some of the outdated systems that we're using right now?

Mr. BITKO. Congressman, there's no doubt that there is the capability in government to deploy sophisticated technology. It happens across many Federal agencies today. I think the question about whether blockchains should be used versus other technologies, it really comes into what's the specific process or problems that's trying to be solved? There are some cases where a blockchain might be a really good fit. There are going to be other areas where it's not necessarily the right thing. I think that it's important for, as IT investments are made, for Congress and for agencies to be careful about not being too prescriptive—right—because there will ab-

solutely be times where, yes, we should use blockchains. But many of these legacy systems that we are struggling with now, they exist because there was some prescriptive requirement or some regulatory requirement or an agency process that was put in place years ago and that the agency is still complying with.

So, every time we do that, that builds onto the complexity that Mr. O’Keeffe was talking about before. So, I think what that means, what I’m saying, is we need to find the right balance of encouraging investment in the right new technologies and the right cases without being so prescriptive that it limits other opportunities down the road.

Mr. CORNELIUS. Congressman, if I may—

Mr. LYNCH. I was actually speaking to the idea of just, you know, a biodefense stockpile where you do have 50 state partners. We’ve got a menu of items that we believe are necessary going from, you know, pharmaceuticals to PPE and it’s—it’s—I don’t know. I just think it lends itself to that blockchain system where multiple parties would be able to have transparency of what is in the stockpile and whether the Federal Government and our states are actually prepared. Right now, the current system is—it lacks all transparency. There’s no accountability.

You know, if you use the Ethereum network, for example, you’re going to have smart contracts that actually, you know, use the Internet of Things to actually order PPE as it reaches its expiration date. Those types of innovations that might be helpful in the biodefense stockpile application, I agree with you wholeheartedly that you can’t just simply say, “OK, use the blockchain for every application and every need.”

But I just thought that the biodefense stockpile, because it is rather static and well-defined, that it might be one of those functions that would actually help government begin to explore some of the new technologies and actually find, you know, government applications that could be served by that technology.

Mr. CONNOLLY. Mr. Lynch, did you want to invite other members of the panel to respond?

Mr. LYNCH. Please.

Mr. CONNOLLY. Ms. Schank or Mr. O’Keeffe.

Ms. SCHANK. Yes, thank you.

I want to reframe the conversation just a little bit because we were talking earlier about the idea that you’re tearing down a bridge and building a new bridge when you think about replacing a legacy system, and I’m not—I think that’s not exactly the right metaphor. So, I just want to put in everybody’s minds the way that technology typically is developed today is to build something small and test it, launch it, and then build on that. So, that when we were talking previously about these multiyear contracts, yes, to replace everything that a legacy system does is likely a multiyear effort, but it could be a couple of months to replace a small piece of that and another couple of months to replace the next piece of that.

So, I think it’s very overwhelming to think about taking an entire legacy system offline and replacing it with blockchain. So, I think that it is a little bit easier to think about what does this thing do and how do we best—how do we make sure, with the current technology, we’re doing that to the best of our ability? And the

way that that—the technology that guides that may change. It likely will change. So, to echo what was just said previously about the—being technology agnostic and not too prescriptive.

Mr. CONNOLLY. I thank you very much.

Mr. LYNCH. Thank you very.

I yield back. Thank you.

Mr. CONNOLLY. I thank you, Mr. Lynch. I thank you for joining us today.

The chair will now recognize himself for five minutes.

Mr. Bitko, could I followup on something you said about FISMA? Let me, first of all, invite your organization, as well as anybody else, to work with us in updating FISMA. I completely agree with you. I think the last time we even authorized FISMA or went through a reauthorization, I was a freshman. It was 10 years ago. So, that's an eternity in technology. So, we—I would invite you very much to be in touch with our subcommittee in reviewing an updated FISMA. I think that's a great idea.

Let me ask you, Mr. Bitko, and you, Mr. Cornelius, and the others could comment as well. We had a hearing last week on the Solarium Cyber Commission, and one of its recommendations was that effectively to create a cyber czar. And while in and of itself that may be a great idea, I am concerned that we have a—OK, now we'll have a CTO; we'll have a CIO; we'll have an information security chief; we'll have a science and technology adviser; and now we'll add a cyber czar. We're trying to, through FITARA, evolve into a primus inter pares where there's one CIO vested with the responsibility for making these investments and making them work, including making sure they're cybersecure.

And I just wonder if you would have any thoughts or concerns to share with us about that kind of management structure.

Mr. Bitko, did you want to comment first? And then I'll call on Mr. Cornelius.

Mr. BITKO. Certainly, sir. Thank you for the question.

In general, I think we support the idea of a cyber czar. There is, I think, a need for somebody who's providing that coordination. The mission, as I understand the cyber czar, is different from the CIO, is different from the chief information security officer. And there is a need and a role for all of those. I do think it's a question about—

Mr. CONNOLLY. Could I interrupt you, Mr. Bitko, though? I mean—

Mr. BITKO. Please.

Mr. CONNOLLY. All right. Let's stipulate that makes sense. But would you not agree that the cyber czar can't do a great deal if he's dealing with 40-year-old legacy systems, that the upgrades we're talking about have to happen to create the predicate of a cybersecure environment? And he or she is not responsible for those investments. The CIO is.

Mr. BITKO. Sir, there's no doubt that there is a close dependency between the cyber czar's piece of the mission that is about the cybersecurity and the investment in legacy systems and modernization and the work that's being done at the OMB-CIO level and at the CISO level. Those things all have to work well together.

I think you're hitting on a point that, in the private sector, this is an ongoing topic of discussion as well. Exactly how all these different entities should be reporting into an organization is the thinking on that continues to change and evolve. You can look at some organizations today where the enterprise CISO, for example, in many large banks doesn't report to the CIO, but it reports directly up to the CEO and the chief operating officer, recognizing the importance of the security mission in and of itself. Even though it's not a cost center in the same way that other parts of the business might be, it's so important to the mission.

I think that some of what I'm saying here is that we need to raise the game of the entire Federal Government and the knowledge of all of our senior leaders about these technology issues, about cybersecurity issues across the board. I think that a way to do that is to have there be somebody who's responsible, looking across all those things. But another way to do it is to realize that the challenge and the mission is so broad here that it's more than a one-person job. Absolutely some work needs to go into figuring out how all those pieces work together or—

Mr. CONNOLLY. I—

Mr. BITKO [continuing]. They won't be successful.

Mr. CONNOLLY. I certainly agree with you.

But when you ask yourself what could go wrong with that kind of nonhierarchical overlapping set of responsibilities to something so important, one is somewhat concerned. It's not like it's worked well up to now. And adding one person vested with cyber has the risk, knowing the Federal Government, of creating a new—with the best of intentions—a new silo. Well, that's her responsibility or his responsibility, not mine. And that is of concern.

Mr. Cornelius, did you want to respond to that?

Mr. CORNELIUS. Thank you, Congressman.

I generally echo Mr. Bitko's comments about the cyber czar. And I would, as I understand the recommendation, one of the responsibilities of the cyber czar would be to help sort of coordinate and understand and oversee budgets for individual Federal agencies when it comes to their own cybersecurity posture but to also do this sort of higher level cybersecurity coordination across FBI, CISO, the IC, other places.

And I do think coordination across these agencies with what I will call sort of—"offense" is not the right word, but sort of outward-facing cybersecurity responsibilities versus agency CISOs, which have internal-facing cybersecurity responsibilities, I do think stronger coordination there could lead to some better outcomes.

Mr. CONNOLLY. Yes. Because we're so good at coordination in the Federal Government.

Mr. HICE. Mr. Chairman? Mr. Chairman?

Mr. CONNOLLY. Yes, Mr. Hice.

Mr. HICE. Just real quickly, I would like to say there are several on our side that would share some concerns. It's certainly an issue that needs discussion and needs to be worked through, but there are certainly as well some very serious concerns. We would be happy to work with you as we go through this process.

Mr. CONNOLLY. And as you know, Mr. Hice, I share your concerns. It's not that it's a bad idea in and of itself. But how will it

work in the context that exists? And we want it to work. We certainly agree, all of us, that cyber is a growing concern. We know there are cyber-attacks right now as we speak on Western institutions that are trying to develop a vaccine, for example. So, we all understand that. The question is, what's the best way to do it? And I want to make it work. And I know you do as well, Mr. Hice. So, those are shared concerns.

Let me end, if I may, with one more question put to each of you on the panel. Give us a grade for how well, from an IT point of view, the Federal Government has done during this pandemic and economic collapse. And who's your favorite example of either getting it right or kind of not getting it right?

I'm not trying to flail anybody, but I think lessons learned are really important, and I gave some of mine: E-Tran at SBA, some of the IRS failures in terms of getting out the direct payment checks. Certainly, at the state level, the collapse of unemployment systems on an IT basis is very painful to watch and experience.

Mr. O'Keeffe, would you like to start first?

Mr. O'KEEFFE. Thank you, Mr. Chairman.

We executed a program called CIO Crossroads where we interviewed each of the Federal CIOs and asked them for their pandemic experience, and overall, I would give the Federal CIOs an "A" for effort. Everybody was working around the clock to try and make things happen. At the overall level, Suzette Kent did a fantastic job bringing the CIOs together.

Were there challenges in many of the legacy systems? Yes. And what we saw was those agencies that have already made the jump to the cloud were much more effective. And agencies like SBA, which had challenges, I would applaud the work of Maria Roat and Guy Cavallo over at SBA who in the middle of this storm when there were challenges at SBA, managed to have the authority to shut down legacy systems and make hard transitions.

So, I think overall the CIO corps did very well. The agencies have their challenges, and it reinforces the requirement to move to the cloud and also elevates the role of the CIO. So, we need to double down on FITARA.

Mr. CONNOLLY. Thank you.

Ms. Schanks.

Ms. SCHANK. Thank you. I was a terrible student. So, I don't want to give anyone grades, but I will say that—

Mr. CONNOLLY. Oh, come on. We're about to have a hearing next week where we give every Federal agency a grade. Do you want to cop out?

Ms. SCHANK. I think that it's an unfair assessment because, you know, when something isn't working well at a baseline level, going back to the bridge example: If you have a bridge and it does well with everyday traffic, but then suddenly there is 10 times the amount of traffic, it in theory should built to sustain that, but a lot of our tech systems at the Federal level are really only and also at the state level are really only keeping up with—you know, they're barely making it through just the everyday. So, then the pandemic are tenfold.

I will say that the IRS, when after the CARES Act passed, there was a – non-filers were not able to file, and we actually, at New

America, did work to discover that hole. And as soon as we made that public, the IRS did very quickly send out a tool for non-filers to be able to file for the stimulus. So, I will give them credit for that. Should it have occurred in the first place? No. I think that's—yes, thank you.

Mr. CONNOLLY. Well, if I could just add to your point, I mean, we're not trying to lay blame. Let's take IRS. IRS had trouble in part because it experienced over a 10-year period a 20-percent cut in its budget, and it was starved of resources, including IT resources. So, how can one be surprised that, when all of a sudden, we are faced with a pandemic and an economic collapse of almost unprecedented proportions, IRS doesn't have the capacity to respond with the alacrity we would like? That's on us for the resources we deprived it quite consistently over a 10-year period.

So, I'm not trying to give a grade where, you know, we're going to bring them in and flog them before the public. We bear some responsibility, but we need to identify performance, and we can all then argue about or debate about what contributed to that performance.

Mr. BITKO, did you want to comment on what kind of grade you might give the Federal Government in terms of response to these twin crises and any candidate you want to praise or maybe highlight in terms of significant concerns or failures?

Mr. BITKO. So, I would agree with the A for effort comment from Mr. O'Keefe. I think lots of Federal agencies put a lot of hard work in and managed to stay in operations and keep going, and that's, frankly, impressive and probably better than I would have anticipated at the very beginning of the crisis.

I think where the grade is maybe a little bit less good is in the COOP planning that agencies would have been doing beforehand where the COOP planning was based on, you know, post 9/11 or even going back to the cold war era and you need to be out of the immediate D.C. area. So, agencies have warehouses out in West Virginia or out in Virginia where employees would go work and, then obviously it is not a viable situation today and that highlights that some of those planning processes need to really be rethought.

And I think this is a place where agencies and CIOs need to do a better job of integrating that thinking together and understanding the technology is so fundamental to the mission that there are other, better, different solutions than having a warehouse out in the middle of nowhere where you cram a thousand people into it with a bunch of computers.

But I do think that agencies figured out how to get past that, and so that is an impressive recovery, and I will use the opportunity to laud my former agency who was not an agency that was disposed to telework by any means. The mindset definitely was you got to be in office to do the job and telework is the exception only in extreme circumstances. They managed to deploy technologies, leveraging the cloud, leveraging virtual desktops, leveraging modern solutions.

And from what I hear from a lot of my former colleagues now, they're sitting there, saying: Why are we ever even going to go back into the office? We're working so effectively remotely now, which I think is a great thing. I think it puts a challenge on government

agencies for long-term strategic planning when you've had capital budgets based on big facilities and rent for space for the entire work force. Is that the right model going forward?

And I think that's something that is a question Congress should be asking. You know, do we need to plan for it? If the agency has 50,000 employees, 50,000 desks that employees are going to come in and sit at, or can we get by with a lot less than because we delivered successful remote work?

Mr. CONNOLLY. Good point.

And I think, at some point, that's going to be a worthy study in terms of permanent quasi permanent changes post-pandemic and certainly workplace changes are going to be considerable, and I agree with Mr. O'Keeffe. Telework is absolutely going to be a permanent part of the future, looking forward. Whether it replaces all physical work, that's a different matter. I doubt it. But certainly, it's going to be a tool in the kit bag and far more pronounced and commonplace than it has been in the past.

Mr. Cornelius, you get the last word on that question.

Mr. CORNELIUS. Thank you, Congressman.

And I will take your bait and say that I think Congress has actually done a pretty good job of dealing with the COVID response. I mean, you did—

Mr. CONNOLLY. Thank you very much. This hearing is adjourned.

Mr. CORNELIUS. But, in all seriousness, I mean, when this happened you didn't go and just build new hearing rooms. You used WebEx, which is a commercial capability, to do this. Now you're doing a little bit of both. This is what the hybrid hearings are.

But, you know, I think that's a very salient point of how you show from a legacy mindset of, "Well, we can't meet in person; let's go find different ways to meet in person," to, "We've got this great commercial technology; maybe we should use that to have hearings and build records and everything else."

So, I do—and to the executive branch's credit, you know, I think of something like the Paycheck Protection Program. I mean, the SBA was responsible for getting more money than was allotted in all direct spending in the American recovery and investment act out themselves in less time than agencies spent those Recovery Act dollars.

So, you know, obviously doing that is going to cause some complications, but I think SBA acquitted themselves quite nicely, and I think it's because of tremendous leadership at the top of the agency with both their former and current CIO. Investing in cloud, investing in a lot of these modern commercial capabilities, they were able to do that.

And the last point I'll make—and we've talked about this with this sort of funding and everything else—is I think Congress—I think there's a great analogy that's happening right now in the House of Representatives. It's my understanding that you-all are considering the Great American Outdoors Act this week, and I think it's the perfect analogy to what we've talked about with legacy IT. I mean, agencies or, you know, the National Park Service has spent years being underfunded and could not actually go back and invest in all of the upkeep and maintenance they needed to do on park lands. And now Congress has recognized it and said, "All

right; we're going find a way to make sure this is funded going forward so that you can do that."

And I think, one, I commend Congress on that, and I hope that they'll move forward; and, second, I hope Congress takes that same position when it comes to legacy technology. And it will be a different challenge, and it will be more complicated because it crosses all agencies, and it's not just about one individual government—one government program or one agency.

But, you know, I think the only way that we're going continue to learn from COVID and really take the lessons and the good and the bad that are happening right now as we sit here and embrace those challenges and, you know, or overcome those challenges and embrace the opportunities that COVID has provided is to ensure that there's enough funding and enough accountability and enough flexibility for agencies to buy and use commercial technology to deliver better outcomes for citizens. Thank you.

Mr. CONNOLLY. Thank you.

And I would just say one of the questions that did not get asked often enough, quite frankly, in putting together the CARES Act or the HEROES Act, for that matter, is, what's the capacity of the recipient agency to be able to do this? You mentioned SBA. We changed eligibility. We pumped more money into SBA than at least 10 years of its budget in less than 10 weeks. We wanted them to expand financial institutions that could carry those portfolios. We changed, simplified the application, and we were willing to convert it under certain minimum circumstances from a loan to grant. Now what's the capability of reprogramming your system SBA, let alone also monitor this for fraud; for, yes, you're eligible/no, you're not; for determination of amounts; on and on and on?

And the same thing with unemployment insurance. We changed eligibility. We extended the time period. We added \$600 a week. That all had to be reprogrammed in 50 individual systems. And then we broadened eligibility to gig workers, sole proprietors, self-employed. And, of course, again, the volume was enormous.

So, you know, we had 47 million people file for unemployment insurance in this time period, and what we found was individual IT systems in the states were simply not capable of handling the volume or reprogramming the eligibility and the terms. And many of them have legacy systems that still use COBOL, to go back to the late 1970's.

So, we need to pay more attention to both the Federal recipients of Federal money and the state recipients, if we're concerned about efficacy and making sure that we're minimizing the pain out there that we're trying to address. IT is integral to that. It's not kind of a sideshow that we can get around to.

So, anyway, I thank all of my panelists. I thank my colleagues for making today possible.

And, Mr. Bitko, don't forget the invitation to talk to us about FISMA.

Mr. BITKO. Can do. Thank you, sir.

Mr. CONNOLLY. OK. All right.

So, without objection, all members have five legislative days within which to submit additional written questions or material.

Further, witnesses through the chair will forward those to the witnesses and would ask for their speedy response.

With that, this hearing is adjourned.

[Whereupon, at 3:40 p.m., the subcommittee was adjourned.]

