AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

TO THE CLOUD! THE CLOUDY ROLE OF FEDRAMP IN IT MODERNIZATION

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JULY 17, 2019

Serial No. 116–48

Printed for the use of the Committee on Oversight and Reform



Available on: *http://www.govinfo.gov*
http://www.oversight.house.gov or
http://www.docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
37–585 PDF WASHINGTON : 2019

COMMITTEE ON OVERSIGHT AND REFORM

ELIJAH E. CUMMINGS, Maryland, *Chairman*

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

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

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

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

GERALD E. CONNOLLY, Virginia, *Chairman*

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

MARK MEADOWS, North Carolina, *Ranking Minority Member*
THOMAS MASSIE, Kentucky
JODY HICE, Georgia
GLENN GROTHMAN, Wisconsin
JAMES COMER, Kentucky
RALPH NORMAN, South Carolina
W. GREGORY STEUBE, Florida

C O N T E N T S

Page

Hearing held on July 17, 2019 1

WITNESSES

PANEL I

Anil Cheriyan, Director, Technology Transformation Services General Services Administration

Oral Statement 4

Jack Wilmer, Deputy Chief Information Officer, Cybersecurity, U.S. Department of Defense

Oral Statement 6

Joseph Klimavicz, Deputy Assistant Attorney General and Chief Information Officer, U.S. Department of Justice

Oral Statement 7

Jose Arrieta, Chief Information Officer, U.S. Department of Health and Human Services

Oral Statement 9

PANEL II

Douglas Barbin, Principal, Schellman & Company, LLC

Oral Statement 22

Jonathan Berroya, Senior Vice President and General Counsel, Internet Association

Oral Statement 24

Will Ackerly, Chief Technology Officer, Virtru

Oral Statement 25

Lynn Martin, Vice President of Government, Education, and Healthcare, VMware

Oral Statement 27

The written openning statement and the witnesses' written statements are available on the U.S. House of Representatives Repository at: https://docs.house.gov.

INDEX OF DOCUMENTS

The documents listed below are available at: https://docs.house.gov.

* QFR's: from Chairman Connolly.

* QFR's: from Rep. Meadows.

* QFR Responses from: Will Ackerly, Chief Technology Officer, Virtu; Douglas Barbin, Princeipal, Schellman & Company, LLC; Jack Wilmer, Deputy Chief Information Officer, U.S. Department of Defense; Lynn Martin, Vice President of Government, Education, and Healthcare.

TO THE CLOUD! THE CLOUDY ROLE OF FEDRAMP IN IT MODERNIZATION

Wednesday, July 17, 2019

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

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

Present: Representatives Connolly, Norton, Lawrence, Khanna, Meadows, Massie, Grothman, and Steube.

Mr. CONNOLLY. Thank you.

The subcommittee will come to order. And without objection, the chair is authorized to declare a recess of the committee at any time.

The subcommittee is convening regarding the role of FedRAMP in IT modernization, with the intention to introduce legislation to codify the program. This hearing will inform that legislation.

I now recognize myself for an opening statement.

I want to welcome everyone here to the hearing on the topic of cloud computing, specifically Federal acquisition of secure cloud computing services. Cloud computing has the potential to help agencies modernize their information technology, while saving taxpayers money, by eliminating the cost to the government of building, operating, and maintaining those IT products themselves.

The Federal Risk and Authorization Management Program, known as FedRAMP, was established in 2011 to provide a standardized governmentwide approach to security assessment authorization and continuous monitoring of cloud computing services. In short, FedRAMP is supposed to reduce the redundancies of Federal cloud migration.

Recognizing the potential of cloud computing, the previous administration established FedRAMP with the goals of reducing duplicative efforts, inconsistencies, and cost inefficiencies with the security authorization process; establishing a private-public partnership to promote innovation and the advancement of more secure information technologies; using an agile and flexible framework that will enable the Federal Government to accelerate the adoption of cloud computing; creating transparent standards and processes for security authorizations; and allowing agencies to leverage security authorizations on a governmentwide scale.

Unfortunately, since the program began, cloud service providers, some of whom are our constituents, have expressed concerns re-

garding FedRAMP's efficiency, effectiveness, and transparency. These stakeholders have noted that the process to become FedRAMP certified can be expensive and time consuming. What was supposed to be an expedited process, six months, may be costing a quarter of a million dollars, instead, in many cases, took years and takes years and can cost companies millions of dollars, the very opposite of what FedRAMP was designed to achieve.

In an audit of the FedRAMP program management office's goals and objectives, the General Services Administration Inspector General found that, while FedRAMP PMO has taken action to address some of these concerns, additional action is needed to strengthen the PMO to better meet the needs and requirements of the program.

Last month, the Trump administration issued its Federal Cloud Computing Strategy called Cloud Smart, which reaffirmed the administration's support for FedRAMP. While acknowledging that the FedRAMP program management office has made improvements to the program and has reduced the amount of time it takes to authorize a cloud service provider in most cases, the policy also notes there's still a lack of reciprocity across agencies in adopting FedRAMP authorizations, which has led to significant duplication of effort when assessing the security of a cloud service offering.

The policy also notes that a large number of agency-specific processes has made it complicated for agencies to issue an authorization to operate for cloud services, even when a cloud service provider has already been authorized at other agencies. And that is a concern the ranking member and I have shared for the last two Congresses.

The Federal Government must do better when it comes to acquiring cloud computing technologies. We cannot afford to repeat the siloed processes of past IT acquisitions that's led to spending $90 billion annually, a large chunk of which is on maintaining legacy systems. However, we can't leverage the potential of cloud computing if the processes are slower than the speed at which the technology itself advances.

In a report published in April of this year, the GAO analyzed IT dashboard data of 16 agencies to evaluate those agencies' use of cloud services for fiscal years 2016 through 2018 and projected use in 2019. In Fiscal Year 2016, those 16 agencies reported 8 percent of their IT investments, on average, used cloud services, with that average projected to increase by 11 percent in fiscal 2019. Some agencies, such as Social Security and GSA, projected nearly 40 percent of their total IT investments would be for cloud computing services, a 100 percent increase.

As more of the Federal Government continues to increase its investment in cloud computing, I believe we can achieve the original goals laid out for FedRAMP. Last year, the ranking member, Mr. Meadows, and I introduced legislation to codify the program and to enable wider agency reuse of existing authorizations to operate. We're working on legislation together this year that would maintain those two objectives while also helping to improve the program by increasing the use of automation and providing for more transparency, all while continuing to ensure that cloud computing services are secure for use by Federal agencies.

The bill establishes a presumption of adequacy for those security assessments that have been FedRAMP-certified to increase agency reuse of authorizations. It requires FedRAMP to establish and make public metrics on the length and quality of assessments and to report progress toward meeting those metrics to Congress. It calls on FedRAMP to find ways to automate the process to increase the efficiency of security assessments.

I hope those are all needed improvements we can agree on, and that includes the Trump administration. I don't often say it, but I think we're on the same page.

I want to thank all of our witnesses for coming to today's hearing. I look forward to hearing from them about the current state of FedRAMP and how the process could be improved and about the future of cloud computing in the Federal Government.

And with that, I call upon my good friend, the distinguished ranking member from North Carolina, Mr. Meadows, for his opening statement.

Mr. MEADOWS. Thank you, Mr. Chairman.

Thank all of you for being here.

Mr. Chairman, I just want to highlight your leadership in this area and truly how you've worked, not only in a bipartisan way, but you have been very inclusive on this issue that is critical, and I just want to say I thank you for that.

Obviously, as we look at FedRAMP and what it is and what it is not, it's all about providing agencies state-of-the-art transformative power, and yet what we've—as the chairman has highlighted, going back all the way to 2011 when the first cloud, Cloud First initiative was first introduced, and as he mentioned, the Cloud Smart announcement earlier this year, it is critical that we are all on the same sheet of music and that we are rowing in the right direction.

And I think probably the frustration for me many times is that the Federal Government that spends over a hundred billion dollars a year on IT is so lagging behind the private sector. I can get—I can have cloud computing in a secure environment much quicker than it seems like some of our Federal agencies. And that's not to be condemning of anyone here or any of you, because I think from your nodding you share my concern. And yet what we have to do, as the chairman highlighted, is make sure that we take these same efficiencies that are available to both the private and public sector and make sure that it's not laborious in its implementation.

We've had great successes with the pilots and where we are now, and as the chairman mentioned, we're working on legislation again this Congress to try to make sure that, not only is it codified, but that we take some of the stumbling blocks, as the chairman mentioned, some of the implementation, it just needs to go faster.

I was at OPM the other day, and we were looking at some of their systems and what they had to go through to actually just do basic functions that I could probably do on an iPhone now, and yet we've got these legacy systems that—and they have to go in and log in and out of so many different systems to get something that, honestly, if it was in the clouds, we would have access to all of that where we would be able to ping it from multiple locations.

But this is all about making sure that we have great cybersecurity as well. And so I don't want us to be fast and yet run into some of the same cybersecurity concerns that we have been plagued with under the legacy systems that we have already.

You know, the FedRAMP has worked with over 150 agencies, 220 cloud providers, and saved over $250 million. That's a great story to tell. And we've seen the growth of this growing at some 33 percent each year, and yet some of those benefits still need room for improvement. And so what we want to hear as a committee in a bipartisan way is how can we improve it, how can we codify it, and how can we make it so that agencies, when they make this decision, it gets done quickly. And so anything we can do to streamline that process is great.

I look forward to working with all of you and the chairman on this topic. You know, he said he wants to, you know, reach for the clouds, and I think it's time we ramp it up. How about that? All right.

I yield back.

Mr. CONNOLLY. I thank my good friend. And I want to thank him for being a great partner for a number of years on the whole information technology management challenge in the Federal Government. We've worked together in a bipartisan basis on FITARA, on MGT, on the sunset provisions of FITARA and now on FedRAMP, and we're going to continue that bipartisan tradition on this subcommittee, on this subject for sure.

We now have a panel of four members. We have Anil Cheriyan, the director of Technology Information Services at GSA, the General Services Administration; Jack Wilmer, the deputy chief information officer for Cybersecurity at the Department of Defense; Joseph Klimavicz—is that right?

Mr. KLIMAVICZ. Klimavicz.

Mr. CONNOLLY [continuing]. Klimavicz, deputy assistant attorney general and chief information officer at the U.S. Department of Justice; and Jose Arrieta, chief information officer at the U.S. Department of Health and Human Services.

If you all four would stand and raise your right hand to be sworn in. It is our custom to hear sworn testimony in this committee.

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

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

The microphones are sensitive. So if you'll speak directly into them like I'm doing, you can be heard.

And we'll begin with you, Mr. Cheriyan.

STATEMENT OF ANIL CHERIYAN, DIRECTOR, TECHNOLOGY TRANSFORMATION SERVICES, GENERAL SERVICES ADMINISTRATION

Mr. CHERIYAN. Thank you.

Chairman Connolly, Ranking Member Meadows, and distinguished members of the subcommittee, good morning, and thank you for the opportunity to testify here.

I am Anil Cheriyan, deputy commissioner of the Federal Acquisition Services and director of Technology and Transformation Services within the GSA. Prior to joining the GSA in January of this year, I served as a CIO at SunTrust Banks, where as part of the executive leadership team, I led digital, data, and operational transformation for various parts of the bank. Also in my SunTrust role, I led a sectorwide committee on cybersecurity standards, and so I understand the criticality of this program for government.

I joined TTS because I was attracted to its mission of making the lives of the American public better by leveraging technology. FedRAMP, I believe, is an integral part of this mission. At its core, the value proposition of FedRAMP is threefold. One, it's about creating a single—leveraging a single consistent standard for authorizing cloud products to improve the security posture of Federal Government. Two, it's to allow cloud service providers and agencies to have an authorization in a streamlined, cost-effective manner. Three, it's to encourage the reuse of these authorizations across the Federal Government, thereby saving effort and cost on the part of agencies and the industry.

I've been at the GSA for a little over six months now, and I'd like to share with you some of my initial observations and thoughts on the future.

I believe FedRAMP is turning a corner and is on the path to success. FedRAMP provides tremendous value to both government and industry. While the process has evolved over time and some of the improvements have shown great results, there's still opportunities to further improve FedRAMP's performance.

Prior to its inception in 2012, agencies issued their own authorizations to operate, using their own standards, and the FedRAMP process was established to create a common authorization process that can be used across Federal Government.

The program has made several improvements based on industry feedback, frankly, with program additions such as FedRAMP Connect, FedRAMP Ready, FedRAMP Tailored, FedRAMP Accelerated. In addition, we have increased outreach to agencies and cloud providers. Let me highlight some of the outcomes of these process improvements.

So after a relatively slow start where it took three years to authorize 50—40 products, we authorized 40 products in 2018 alone. As of today, there's 143 products authorized, with nearly 70 in the pipeline. We've decreased timelines by almost 50 percent, with authorizations taking, on average, 5–1/2 to eight months. In the last two years, the number of agencies have grown by roughly 40 percent to 156 agencies. And reuse has grown as well, with the average reuse of eight times. On some cases, in some instances, some products are reused over 150 times. We believe this has saved agencies and industry over $285 million in cost avoidance.

So while—as I mentioned before, while these improvements are great, there are still real opportunities to show improvements. So looking ahead, I plan to leverage my prior industry expertise and continue to drive improvements, working in close partnership with industry and agencies.

And here are some immediate short-term improvement opportunities that we've already embarked on. In order to better channel

the feedback from industry and agencies, we will participate in the recently established ACT-IAC FedRAMP working group. Second, we will further streamline processes and automate processes and workloads, as well as evaluate a threat-based approach to authorization. In addition, we will expand our industry and agency training to further clarify any process concerns.

I'm sure we'll come up with additional opportunities, but this is by no means the sum total of all opportunities. There's significant opportunities as the process improves and evolves further.

So I'd like to summarize by saying I believe FedRAMP is turning the corner and it's on the path to success. And I'm committed to work in close partnership with industry and agencies to continue to make improvements.

Again, thank you, and I look forward to the opportunity to obtain your feedback and answer any questions.

Mr. CONNOLLY. Thank you, Mr. Cheriyan.

And by the way, in drafting our bill, we had very useful input from your colleagues at GSA and they were productive and helpful, and we appreciate that.

Mr. Wilmer.

STATEMENT OF JACK WILMER, DEPUTY CHIEF INFORMATION OFFICER FOR CYBERSECURITY, U.S. DEPARTMENT OF DEFENSE

Mr. WILMER. Good morning, Mr. Chairman, Ranking Member Meadows, and distinguished members of the subcommittee. Thank you for this opportunity to testify today on the effectiveness of the Federal Risk and Authorization Management Program, FedRAMP.

I am Jack Wilmer, the deputy CIO for Cybersecurity and the chief information security officer for the Department of Defense. I also serve by delegation from the DOD CIO as one of the three chairs of the FedRAMP Joint Authorization Board.

Today, I will provide background on DOD's participation in FedRAMP, the effectiveness of FedRAMP, and the synergy between DOD and the FedRAMP Program Management Office to provide authorization for cloud services for the Federal Government.

DOD has been a partner in the FedRAMP program from its inception, and our involvement has been a major benefit to the Department. We have leveraged FedRAMP to make about 140 cloud service offerings available for use in DOD thus far.

DOD supports the FedRAMP program by providing technical assessments and continuous monitoring support and by providing strategic programmatic support and oversight through the Joint Authorization Board.

The FedRAMP JAB is a critical collaboration venue for improving cloud cybersecurity practices across the Federal Government, and provides efficiency through the issuance of JAB Provisional Authorizations to Operate, or P-ATOs, to cloud service providers.

A JAB P-ATO allows the Federal Government to evaluate cloud service offerings once and reuse many times. Federal mission owners leverage the risk information enumerated by the JAB in the P-ATO, and as of June 1, 2019, there have been over 722 reuses of JAB-authorized services, resulting in over $180 million in cost avoidance.

DOD provides full reciprocity for cloud service providers who have been granted a FedRAMP moderate authorization for use with DOD public data. However, as a result of the threats which routinely target DOD systems, we require cloud providers to meet cybersecurity requirements specified by the Committee for National Security Systems to be able to process any DOD-controlled unclassified information. These additional requirements only add 38 controls to the 325 required for the FedRAMP moderate baseline.

We issue a DOD provisional authorization to systems that have met our requirements, and this process adds one to six weeks to the FedRAMP certification process, depending on the sensitivity and complexity of the system. We have issued 120 provisional authorizations through reciprocity with the moderate baseline and have only had to require additional DOD assessments for 20 cloud services.

As the Department continues its transition to the cloud, it is becoming more important to increase the speed of authorizations for new cloud capabilities. One upcoming change for DOD is that we will now issue a general provisional authorization which will cover any cloud service offering which has been assessed at the FedRAMP moderate baseline. This means that cloud service providers will not have to wait for a separate DOD authorization to have their services used for DOD public data. This use case covers the vast majority of DOD provisional authorizations that have been issued to date, and we expect to make this change within a month.

We continue to review opportunities to improve authorization timelines through communication with vendors and the interagency stakeholders, and we strive to achieve as much consistency as possible between the FedRAMP and DOD security control baselines.

I would like to emphasize the importance of FedRAMP and the standardized approach the program provides for cloud products and services. This approach saves money, time, and staff required to conduct the Department's security assessments.

Thank you for the opportunity to testify this morning, and I look forward to your questions.

Mr. CONNOLLY. Thank you, Mr. Wilmer.

Mr. Klimavicz.

STATEMENT OF JOSEPH KLIMAVICZ, DEPUTY ASSISTANT ATTORNEY GENERAL AND CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF JUSTICE

Mr. KLIMAVICZ. Good morning, Chairman Connolly, Ranking Member Meadows, and distinguished members of the subcommittee. Thank you for your continued commitment to improving information technology across the Federal Government, and thank you for the opportunity to appear today before you as the chief information officer at the Department of Justice.

This testimony provides an overview of the Department's use of FedRAMP, some possible areas of improvement, and some considerations for the Federal Government as we begin shaping the next iteration of FedRAMP.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based products and services. The FedRAMP process allows the Depart-

ment to efficiently implement cloud solutions in a secure, cost-effective manner.

To date, the Department of Justice takes advantage of 18 JAB-authorized Provisional-ATOs and 9 ATOs sponsored by other agencies. The Department has also sponsored nine ATOs which can be used by other agencies. Additionally, the Department incorporates FedRAMP requirements into our acquisition policy and contract language. Awarding contracts with this language holds vendors accountable for implementation of security controls.

But like any government program, there are opportunities to improve. So one of the stated goals of FedRAMP is to promote the reuse of Provisional-ATOs and to reduce administrative and cost burdens for both cloud service providers and Federal agencies. But many cloud service providers, especially those unfamiliar with Federal cyber requirements, do not know which security controls to prioritize and implement. Also, the predominantly manual 3PAO assessment process results in less than standardized outputs and lengthened review times.

The cloud has opened up many new methods for small companies to develop disruptive technologies at lower cost. Opportunities exist to support their understanding and implementation of security requirements in a more automated and cost-effective manner. In addition, agency-level ATOs can be difficult to share because of residual risks from tailored or risk-accepted controls that are inherently different between entities. Furthermore, the residual risks are not consistently documented.

FedRAMP also fails to address all Federal security mandates.

Finally, the Federal FedRAMP authorizations do not eliminate all agency assessment, authorization, and monitoring activities. Agencies must still assess controls not implemented by the cloud service provider, as well as provide for FISMA-required continuous monitoring of those same cloud-based services for the entirety of their operational life cycle.

As the Federal Government and its partners shape the next iteration of FedRAMP, I'm glad to offer a few observations for improvement. First, an automated security assessment methodology could be developed to allow third parties to assess cloud service providers in real time. This would produce a cyber risk—security risk score for Provisional-ATOs, reducing the cost and time investment of services—service providers.

Second, replacing the manual 3PAO review with real-time assessment platforms based on technical measures, machine output only, and issuing Provisional-ATOs based upon risk scores will eliminate the long wait times for manual review by the FedRAMP PMO.

Third, require the cloud service providers to use and conform to DHS' CDM standards for continuous monitoring to increase threat awareness, enable consistent cyber reporting.

Fourth, require an independent Federal entity, for example, the Federal CIO Council, Federal Chief Information Security Officers Council, to review JAB Provisional-ATOs to ensure standards are consistent with Federal policy updates.

Fifth, establish standardized acquisition clauses through the Federal Acquisition Regulatory Council to capture Federal Government policies and mandates.

As you can see, FedRAMP is a critical part of implementing the Department's IT modernization efforts, and the Department looks forward to working with the subcommittee, the FedRAMP PMO, the Office of Management and Budget on the next iteration of FedRAMP.

Thank you again for the opportunity to appear before you today. I welcome your questions. Thank you.

Mr. CONNOLLY. Thank you.

Mr. Arrieta.

STATEMENT OF JOSE ARRIETA, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. ARRIETA. Good morning, Chairman Connolly and Ranking Member Meadows and members of the committee. Thank you for providing me the opportunity to discuss the Department of Health and Human Services' FedRAMP program with you today. I appreciate the opportunity to speak with the subcommittee today to share our perspectives on a program that we believe is a strategic enabler for modernization.

I joined HHS 18 months ago, and I was appointed as the permanent chief information officer about 50 days ago. And although I've had a brief tenure as CIO, I'm keenly aware of the value and importance of leveraging cloud technology to drive greater data sharing, greater data security, and greater financial savings.

Why do we look at FedRAMP as a strategic enabler? HHS deals with the most critical information regarding one in three Americans. FedRAMP is the fulcrum for modernization efforts, and we've committed to it.

In 2013, HHS was the first agency to sponsor a cloud service provider through the FedRAMP process. To date, HHS has authorized a total of 14 cloud service technologies and leverages over 60 FedRAMP-authorized cloud products across the enterprise.

We support the standardization and reuse model. It has saved HHS, its customers, and industry countless hours.

At HHS, FedRAMP's success is built on partnership between industry and government. At HHS, FedRAMP is more than a point in time authorization of a specific technology. We actually meet with our industry partners on a monthly basis and share security concerns. This allows us to have ongoing monitoring and maintenance of our FedRAMP-approved cloud service providers.

I thought for a second I would talk to you about the legal framework that y'all have put in place that is actually driving change within Federal agencies and how it's impacting behavior specifically within HHS. To us, FedRAMP is a secure cloud. FITARA is empowering the CIO and giving him the visibility to actually drive change to that secure cloud environment, and the MGT Act is the incentives that actually drives those actions.

An example of this behavior in HHS that we believe will be transformative for the acquisition function is called HHS Accelerate. We thought to ourselves at HHS, wouldn't it be amazing if we could give the cancer researcher that comes to HHS insight on

all of the expenditures associated with cancer researchers that came before him so that he had the benefit of that information in real time available to him at his fingertips so that he could do a business plan or an acquisition plan to spend the money that he has to solve a large problem of cancer? We thought, wouldn't it be amazing at HHS if we could give contracting professionals the terms and conditions and prices paid associated with different products and services from the $24.2 billion we spend every year in the hundred thousand contracts?

It's kind of like going to Target. If you walk in Target and you show them a price that you found on Amazon, the cashier will immediately give you the discount.

Well, because of the legal framework that you've put in place, we've actually been able to build a program which we call HHS Accelerate that we think will facilitate those behaviors. We built that program from April 17 to December 10, and we're testing it now. And we would not believe—we do not believe it could have happened that quickly without this legal framework. So thank you for your visionary work.

All of the work to actually develop HHS Accelerate was performed by small businesses. I've been committed to the small business community as an employee at the Treasury, as an employee at the Department of Homeland Security, and now as an employee at HHS. And I just got an invite to participate in the congressional meet and match procurement workshop conference in September and, if Ethics approves, I'm delighted to attend.

As with anything, there are future opportunities, and I just want to highlight a couple. At HHS, our Secretary and Deputy Secretary have set a goal to make data available to private sector healthcare companies to improve health outcomes for the American people. We call it liberating data. FedRAMP is the mechanism that will ensure that we can securely share data with industry partners that specifically operate in the private sector healthcare marketplace to improve health outcomes for the American people.

We have to educate those companies on what FedRAMP is. They've never done business with the U.S. Federal Government before, but in order to access our data, they need to be a FedRAMP-approved provider. That is extremely important to us, and that is an opportunity to directly impact the American citizens in this Nation. So we believe that education and engagement with the industry base is the single most important criteria for making FedRAMP successful.

I'll close by saying this: At HHS, we believe technology modernization is iterative and evolutionary. As we build, we learn. As we learn, we mature. As we mature, we implement. And as we succeed, we scale. And we've taken that approach. As you guys have built the legal framework to drive change in this marketplace, I think you've taken the same approach, and we certainly appreciate that at HHS.

Happy to answer any questions that you may have.

Mr. CONNOLLY. Thank you, Mr. Arrieta, for your refreshing testimony. And your comments about our legal framework and praising FITARA and our visionary leadership I think merit you a promotion and a big raise on a bipartisan basis. We agree.

The chair now recognizes the distinguished Congresswoman from the District of Columbia, Ms. Norton.

Ms. NORTON. I thank you very much, Mr. Chairman. And could I congratulate you both as well. I love this spirit of self-congratulation.

Mr. MEADOWS. We're very good at it.

Mr. CONNOLLY. Yes, don't spoil it, Eleanor. Come on.

Ms. NORTON. I'm trying not to, but the whole point of this hearing is to see how we can improve FedRAMP.

So I'm going to try to break the spirit just a little bit, because I am interested in the issue of reciprocity. It's a great big Federal Government.

The whole point, I thought, of FedRAMP is to be able to deal across agency lines and that that would be a big incentive for agencies, and yet the reports to this committee is duplication of efforts continue in assessing cloud products. Many agencies have their unique processes and apparently are not lured by reciprocity.

I've really got to—I don't know what—the chairman said 18 percent use FedRAMP. Is that the figure, Mr. Cheriyan, 18 percent of agencies?

Mr. CHERIYAN. Yes. We have about 156 agencies engaged in FedRAMP.

Ms. NORTON. So I'm trying to see what percentage of agencies that is now. You have any idea?

Mr. CHERIYAN. I could get you that number.

Ms. NORTON. I can't do the math because I don't know how many agencies there are, and that might include all kinds of small and large agencies.

And I congratulate you on what you've done. And you listened to what needs to be done and you take action, and it appears to produce some response. So I'm trying to find out the reluctance of the chief information officers to use FedRAMP, even certified products, particularly granted by other agencies.

I guess I should speak with you, Mr. Cheriyan, because you oversee the whole FedRAMP office. Is there more that could be done to get reciprocal trust so that you could—we could speed up the use of FedRAMP? And what—is it just doing things the way they've always done it? I'm trying to get to the root of the problem to find out what the solution is.

Mr. Cheriyan.

Mr. CHERIYAN. Thank you for that question. And as you mentioned, reuse is very important to us. That's one of the core principles of FedRAMP, and that's why it was created in the first place. So it's a significant issue for us that we're working on.

As I mentioned earlier, about 156 agencies are currently engaged in FedRAMP. It's close to a 40 percent increase over the last couple of years. And a lot of that has been due to the outreach efforts that have been going on by the FedRAMP teams, as well as the JAB teams, in terms of getting the word out, in terms of educating, in terms of training.

We've held over 12—you know, we've trained over 12,500 individuals in Federal Government, as well as industry, on the process. We have agency-specific training efforts that are underway. We have CISOs, or information security officers, also going through the

training. So training is a big part of it in terms of really educating all of the agencies in terms of what FedRAMP is, deal with any misperceptions, et cetera.

We're also actively participating in forums. I mentioned the ACT-IAC forum that is about to get started, which is the FedRAMP working group. That is a significant group that we believe we can have a lot of sharing, not only between agencies, but also cloud service providers. We really——

Ms. NORTON. Before my time runs out, it seems to me that the kind of outreach you're doing is appropriate, and that you're listening and responding. So here is my question. It seems to me with these agencies—and, again, I ask the chairman to find out what percentage. I don't know where I got the 18 percent. It may have been from your opening remarks. I know the figure sticks in my head.

But this is a question for everybody. It looks like there need to be incentives given for FedRAMP to encourage agencies to serve as sponsors for cloud providers, and I wish you'd think about that. The outreach seems to be good. The response seems to be good. So this is a question for the entire panel.

If you had to say, now, what could disengage people from what they do already, what incentives could we offer that would make it so attractive that they'd want to, in fact, engage the FedRAMP program? What would each of you say?

Mr. CONNOLLY. The gentlelady's time has expired.

But, Mr. Wilmer, you are authorized to respond.

Mr. WILMER. Yes, sir. Thank you.

Ma'am, what I would offer in response to that, from a Department of Defense perspective, is that we are fully committed to reciprocity, and there's a massive incentive for us in having that reciprocal arrangement with FedRAMP. Going through those 325 controls with the moderate baseline as an example, which is something that the FedRAMP program takes on for us, is work that we no longer have to do in order to leverage those cloud services.

I talked a little bit before about the increased security environment, increased threat environment that our DOD services face. And so we do require additional information, but that's all built on top of the good work that FedRAMP has done.

So in terms of your specific question about incentives, I believe that there's already a major built-in incentive from the FedRAMP program in terms of doing that assessment once and allowing for reuse across the government.

Mr. CONNOLLY. I thank the gentlelady.

Thank you, Mr. Wilmer.

Although, just to followup, it's our information that 57 percent of Federal agencies use FedRAMP. And if that's accurate, that still means 43 percent don't. So, yes, what you say may be true, but it hasn't seeped through to the entire Federal family.

The distinguished ranking member is now recognized for his five minutes of questioning.

Mr. MEADOWS. Mr. Chairman, in the interest of time and seeing that you've got a number of members on your side, here's what I would ask all three of—or all four of you to do.

If you will let this committee know the three major obstacles for creating delays for implementation, how we can either help that administratively or help that legislatively. I think the time is critical, and if you will do that and get that to committee, I think that will be well-served.

I just want to say thank you to all of you. If we can implement it at your levels, the rest of—all the other agencies. There are none that are more critical than the four that are represented at the table. And we'll be able to take it everywhere. And so, you know, they're learning by your both mistakes but also your frontier, pioneer kind of way of getting this done. So I just want to say thank you.

And I'll yield back in the interest of time.

Mr. CONNOLLY. Very well said, Mr. Meadows. And would that all Federal agencies have the enthusiasm for change Mr. Arrieta expressed in his testimony. Thank you.

The chair now recognizes the gentleman from California, Mr. Khanna.

Mr. KHANNA. Thank you, Mr. Chair. I will be brief as well.

In the spirit of congratulations, I will note two unique parts of this hearing because of your leadership, Mr. Chairman, and Ranking Member Meadows.

First, it's Congress displaying a proficiency in competency in technology. What a refreshing change. And, second, it is bipartisanship to that end. In the legislation that you and Representative Meadows have offered last Congress, and I expect that you would offer it this Congress, I think will be a tremendous contribution to continuing to improve FedRAMP.

So my question—let me just ask two questions and then have the panel address it so we can get to the other members.

One, what can we do to better allow small businesses access to participate in FedRAMP? And, two, are there areas based on—I imagine you've read the Meadows—the Connolly Meadows, Meadows-Connolly bill. And are there things that you think are important this time to include in that bill?

Mr. CHERIYAN. So, yes, let me start. Thank you for that question. You know, regarding small business, just a high-level overview of where we are, we've got about 33 percent of the authorized products right now are from small businesses. And if you look at the pipeline, it's around 33 percent. So it's a growing percentage over the last couple of years. It's really increased.

However, there's still more opportunity, I believe, to, one, educate small business. A lot of small businesses are unaware of the process itself, the security requirements that we have, and a lot of time is, frankly, wasted when the small business is really trying to figure that out. So, really, the education piece of creating that and that awareness in small business is something that we take very seriously.

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

Mr. KHANNA. Sure.

Mr. CONNOLLY. That's true, Mr. Cheriyan, but that doesn't let us off the hook. No small business can afford to risk millions of dollars and the uncertainty of no guarantee of when they'll be certified.

Mr. CHERIYAN. Right.

Mr. CONNOLLY. And that's a huge problem for small and minority businesses, women, minority, veterans-owned businesses to enter the field. The big players can afford it. The smaller, medium-sized businesses, frankly, have to really look at it. And that's one of the things our legislation is designed to try to alleviate so that there's more possibility for entry.

Without prejudice to the gentleman's time, thank you for yielding.

Mr. CHERIYAN. Yes. Clearly need to add that the speed at which we are authorizing these products for small businesses needs to improve. And we talked a lot about the automation approaches, the level of risk associated with it. And a lot of small businesses run on existing infrastructure that has already been authorized. So there's a significant amount of inherited risk that has been certified already. So there's lots of opportunities, I believe, to improve that.

Mr. WILMER. Sure. I would add only the—I think the most important thing that we can do is driving additional automation into the assessment process. So there's a lengthy set of controls that small businesses and all cloud providers have to be able to implement, and the more that we can enable in terms of automation of going through that set of controls should reduce the burden of actually going through the process and creating the artifacts that are then required for us to assess.

Mr. KLIMAVICZ. I would just say with respect to small businesses, when I've talked to small businesses, one of the things I hear up front is they need more information to help them make a better business decision, a cost benefit. Which controls do I implement? What's important in terms of future business? Do I go after low-, moderate-, or high-impact tradeoffs, the encryption? Everything, all those decisions, they've asked for more information up front so they can make an investment decision, and also how much is it going to cost to implement these controls and are they going to get that paid back down the road. So understanding tradeoffs, getting more information up front.

And with the second part of your question, I agree with Mr. Wilmer here that I think the automation. As I mentioned in my testimony, everything needs to be real time, everything needs to be automated, and that will help the small businesses.

Thank you.

Mr. ARRIETA. And I'll just say about the automation, as the automation is built, if it is built, there should be direct engagement with the small business community as to what you're building. That will actually help them plan to take advantage of the automation that you're building. That shouldn't be here's what we're thinking of building and then asking further feedback. There should be a dialog there that shapes what is built. And I think if you want to include the small business community, as a former small business executive at the Treasury, you have to engage them as you build the solution.

And I agree with the other panelists' comments.

Mr. KHANNA. Thank you. Thank you, Mr. Chairman.

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

The chair now recognizes the very distinguished lady and accomplished Congresswoman from Michigan, our dear friend, Mrs. Lawrence.

Mrs. LAWRENCE. Thank you, Chairman, for holding this, and to the ranking members here.

Mr. Arrieta?

Mr. ARRIETA. Yes, ma'am.

Mrs. LAWRENCE. I want you to know that, I want to be on the record, I agree. We in government, as we embrace technology, as we try to keep pace with this industry, we must sit down at the table and talk and work together. Because so often, our regulation and our pace that—for our approval lags so far behind innovation and advances in technology. So I really agree.

I wanted to ask this question of you, sir. I would like to ask you how the implementation of cloud services has affected the Department of Health and Human Services. Specifically, how did the implementation enable the Department of HHS to accelerate its mission?

Mr. ARRIETA. Well, thank you for the question. I appreciate that. At HHS, we, as I said in the opening testimony, we award about a hundred thousand contracts $24.2 billion in spend flow through those contracts every year.

What we were able to do in a very short time because we had FedRAMP-approved cloud service capabilities is we were actually able to move all of that contracting data to a commercial cloud environment, and then we were able to use an incremental approach to actually rebuilding our business process and partnership with small business to automate many of the functions of the acquisition life cycle.

If we didn't have FedRAMP-approved products to actually build on, the process would have taken a lot longer. So the ability to actually separate data from business process actually gave us the flexibility to modernize our IT systems, while allowing our legacy IT systems to still function and serve the mission but also directly engaging over 3,000 members of the acquisition community over a nine-month period across HHS and allowing them to design the functionality that would drive the best outcome for them.

We had a really strong and robust business plan around that. If you—you know, privately if you wanted to hear that, I'd be happy to come back and share that with you. But we had very specific ROI measures on the basis of process improvement, on the basis of savings at the point of purchase, and on the basis of infrastructure savings that we thought we were able to generate, and we were able to track those investments along the way because we were able to take this incremental approach, separate data from business process, and modernize.

So I think FedRAMP is a key component to that. And like I said, the legal framework that this committee has put in place actually gave us the tools to make the argument that this was a good idea, and we thank you very much for that.

Mrs. LAWRENCE. Thank you so much.

Cybersecurity threats constantly evolve, and while the FedRAMP controls serve as a baseline, we must ensure that these assessments are flexible enough to incorporate changing security threats.

So, Mr. Wilmer and Mr. Cheriyan, how does FedRAMP stand up to the speed with the evolving cybersecurity threats?

Mr. CHERIYAN. At the core of the FedRAMP process, we use a NIST standard for cybersecurity in terms of the level of risk, whether it's low, moderate, or high. And there's a fairly detailed set of controls that NIST has provided that form the basis of the risk assessment of FedRAMP.

As you mentioned, cybersecurity is really fast-moving.

Mrs. LAWRENCE. Yes.

Mr. CHERIYAN. It moves at a pretty fast pace, and that control and that standard is constantly updated. So we work with NIST to give them feedback, and they get the feedback from a lot of the different agencies, and that's how the whole standard has changed. And can it be done faster? Definitely we should be looking at that, but that's——

Mrs. LAWRENCE. But does FedRAMP emphasize the most important security vulnerabilities that our government faces? Mr. Wilmer?

Mr. WILMER. So, ma'am, what I would offer is that a lot of the controls are really a framework for how you would deal with cybersecurity incidents. So you're exactly right, ma'am, that the threat evolves over time. Many of the controls that we require cloud service providers meet ensure that they are prepared to deal with the evolution of threats, as opposed to ensuring that they are protected against specific ones.

And so that combination of making sure that you have basic security practices in place to protect yourself from the threats and then also ensure that you have the right processes and procedures in place to deal with threats or, you know, worst case, if they are actually negatively impacted by a cyber incident, is a critical piece of that.

And then as Mr. Cheriyan mentioned, as NIST evolves the framework itself, the Joint Authorization Board will actually go through and determine if any additional controls need to be added or removed from the FedRAMP baseline.

Mrs. LAWRENCE. Thank you.

Just in closing, I want to be on the record that it's been amazing and just such an honor to share this time in history with an amazing leader like my colleague, Congressman Connolly.

I yield back.

Mr. CONNOLLY. I wish we could give you a promotion and a raise. Thank you so much, Congresswoman Lawrence.

I now recognize myself for questioning.

Let me just say, my interest in FedRAMP was stoked by a friend and colleague, Steve O'Keefe, at MeriTalk. They had a conference up here a few years ago. And I don't know, there were 125, maybe 150 people in the room. And at one point—and there were all kinds of complaints about FedRAMP.

And at one point, Mr. O'Keefe asked everyone to raise their hands on a simple question. How many of you think FedRAMP is working the way it was designed to work? The only hands that went up were Federal officials in the room, like nine of them.

And then he said, well, how many think it's not working the way it was designed? And the other 120 or whatever hands wept up.

I'm looking at this, thinking, are we that disconnected from, in a sense, our client base, right? FedRAMP has clients, and the Federal Government ultimately is the client, but so are the service providers, right, whom we certify. And it just etched in my mind that we've got a problem, and we were reluctant to address it legislatively. We were hoping it would be addressed administratively. And there have been administrative improvements. And certainly, not least under your leadership, Mr. Cheriyan. But problems continue. And we're going to hear from a second panel, and we're going to hear some problems from the private sector in terms of what they experience.

Let me begin, Mr. Cheriyan, with the budget. My understanding is FedRAMP gets roughly $10 million within your agency from the Federal Citizen Services Fund. Is that correct?

Mr. CHERIYAN. Yes, that's correct.

Mr. CONNOLLY. And 25 percent goes to the JAB, and 75 percent goes to your office at GSA.

Mr. CHERIYAN. Let me just clarify a little bit of that. The $10 million is the amount spent by GSA. And DOD and DHS each spend an additional $2.5 million.

Mr. CONNOLLY. Okay.

Mr. CHERIYAN. So it's roughly $2.5 million for JAB and $7.5 million——

Mr. CONNOLLY. All right. And we'll be certainly talking to all of you about this, but Mr. Meadows and I, in the draft bill, are looking at do we need additional resources. A lot of people in the private sector say yes. We're both pecunious gentlemen; but on the other hand, if FedRAMP isn't working the way we want it to work and it needs some adjustment in resource availability, we're certainly willing to look at that in the draft legislation.

It's my understanding, Mr. Cheriyan, that we're doing about 12 certifications, 12 approvals a year. Is that correct?

Mr. CHERIYAN. Yes. There are 12 JAB certifications per year and another 38 or so agency—30-plus agency authorizations. So perhaps maybe two or three years ago, the majority of the certifications were JAB. And, frankly, the whole approach has pivoted a little bit as agencies have got more engaged, and about 75 percent of the authorizations are now agency authorizations, and only 25 percent are JAB authorizations.

Mr. CONNOLLY. But what are—going back to Ms. Norton's question, I mean, I think from, certainly speaking for myself, and most commonsense perspectives maybe, if you get certified at window X, certainly if you get—let's start with JAB. If I'm certified at JAB, I view that as the gold standard, and that ought to be good for me to punch my dance ticket at all the other windows, except for compartmentalized, highly specialized needs. The idea that, no, that's fascinating, that's our referendum but you've got to start all over again is unacceptable and leads to absolutely needless expense.

And, again, going back to the small minority—small and medium-sized businesses, minority and otherwise, it de facto discriminates against them. They cannot incur that kind of expense. And we have many, many Federal contractors who serve many different Federal agencies.

And so if we're sort of diffusing the approval process, is that forcing businesses to get 24 stamps or 12 stamps, or can they get one with the presumption that's going to be pretty much good, with a few exceptions, at the other windows as well?

Mr. CHERIYAN. Yes, let me take a shot at it and then have some of my colleagues answer.

So just a couple of things. The JAB authorization or an agency authorization, for the FedRAMP PMO standpoint, we view it as the same. It's following the same processes, the same standards, et cetera. The JAB is really using the DOD, DHS, and GSA security leaders to do the authorization. In addition, we provide continuous monitoring, et cetera.

Mr. CONNOLLY. I want to give you a chance to be very clear. You're not arguing JAB is just no different than any other Federal agency. JAB is a different—I mean, it—we created it as a multi-agency entity for a reason.

Mr. CHERIYAN. No. I do believe that the JAB authorization enables a cloud service provider to go to more agencies. So——

Mr. CONNOLLY. That's right. I just wanted to clarify what you were not saying.

Thank you.

Mr. CHERIYAN. The second point I'd make is that when an agency takes a P-ATO from JAB, they don't have to start from scratch. What they're doing is they're looking at whatever the number of the controls are, whether it's low, moderate, or high, and it's a hundred to 300 to 400, depending on the severity or the risk. They will then evaluate on their own risk profiles as to which areas they need to spend more effort in. And so it's not a start from scratch. It's purely a, what has the JAB provided? Do we accept it or do we now need to do more? And that's fundamentally the reuse process that——

Mr. CONNOLLY. Well, let me just say, yes, that's how it should work. But I'm aware of, for example, right now, one entity, a private sector entity that is using a software application that's been approved, that's certified; but because it's for a different application, same software, they have to go through the process, and they have no idea when it will be approved.

Mr. CHERIYAN. Okay. So we should——

Mr. CONNOLLY. And that's millions of dollars and multiple years for a medium-sized, maybe small-to medium-sized business, and that's maddening to people. Like, well, if Mr. Wilmer thought it was okay to use the software, the fact that I'm applying it to HHS, it's the same software, shouldn't the presumption be that, of course, I'm certified, just a different application?

Mr. CHERIYAN. We believe it should.

Mr. CONNOLLY. Okay.

Mr. CHERIYAN. And if there's misperception and——

Mr. CONNOLLY. All right. Expect a phone call.

Mr. CHERIYAN. We're happy to take the phone call.

Mr. CONNOLLY. No, I—thank you.

Mr. CHERIYAN. Yes.

Mr. CONNOLLY. There are going to be hiccups, but what I'm trying to establish is we agree on some principles here that, moving forward, especially once we have a bill, will, in fact, streamline the

process and make it more, you know, user-friendly for people who apply.

Now, let me just ask one more question about the 12 JAB. And maybe, Mr. Wilmer, you want to get in on this. Does that create a backlog? I mean, if we're doing 12, how many are we not getting to every year?

Mr. WILMER. Sir, as you are well aware, there are tons of cloud service offerings, especially when you look at the software as a service space. And that's where, to your point, there is absolutely a backlog of those that would like to go through the JAB process. We do have a published prioritization process through which we determine which order we will actually work through cloud service providers, but that's where I'd also like to give the FedRAMP PMO a lot of credit for coming up with the agency authorization process.

And, really, what this particular capability does is it allows a cloud service provider that has a customer that wants to use it. So any Federal agency can go through and perform an assessment on that cloud service offering. They can then package up all of the work that they did, provide it to the FedRAMP PMO. The FedRAMP PMO can review it, ensure that it meets the standards, and then put that out on the FedRAMP marketplace so that they can still benefit from the same reciprocity that is otherwise offered.

Mr. CONNOLLY. One of the concerns we have is entry into the market. And we've heard people say, through the grapevine, that certain officials of the Federal Government actually want to de facto limit the number, because it's easier to manage how many people are certified and qualified to provide cloud services. And I understand that but, on the other hand, it's a big Federal market, huge.

Mr. Arrieta just talked about how many contracts and how much cumulatively they add up to, and we want to give Americans who are entrepreneurs an opportunity to compete in that market. And sometimes the smaller entities are more nimble and more innovative, depending on the need, and we don't want to find that there are artificial barriers to entry by virtue of a fixed number in our minds or in our willingness or ability to approve. So that's our concern about 12. It seems like a small number.

Mr. WILMER. Yes, sir. So the number 12, part of the impact of going through a JAB authorization is that we are also responsible for the continuous monitoring of the cloud services that we authorize. So as we approve more services, there are more that we have responsibility for ensuring that they continue to meet the standards through which we assess them.

I agree completely with your point in terms of reciprocity, and also your comment about the number of services that we are able to process, but that's effectively part of the limiting reagent that we have in terms of the bandwidth we can support.

Mr. CONNOLLY. Two more questions, and then I'll be finished, and we will thank you so much, and I know we will be in touch again.

One is to you, Mr. Wilmer. You serve on the JAB, representing the Pentagon.

Mr. WILMER. Yes, sir.

Mr. CONNOLLY. In the past, we've had stories told about a private-sector entity that went to the JAB, got approved, and then went to one of the windows at the Pentagon, only to be told, "That's fascinating; you have to apply all over again," as if the JAB thing was advisory or fascinating but irrelevant.

Can you assure us that this no longer occurs, if it did?

Mr. WILMER. Frankly, yes, sir. So I can't speak to the past incident, but what I can tell you is that we have contracting clauses, as an example, that requires a DOD authorization. The process that we use for granting a DOD authorization builds on FedRAMP. So FedRAMP is core to our process for authorizing use of cloud services——

Mr. CONNOLLY. But you work at the Pentagon, and you know that stovepiping is built into the culture.

Mr. WILMER. Yes, sir.

Mr. CONNOLLY. So "How fascinating that the Navy thinks you're certified, but here at the Army we have a very different point of view, and you'll start all over again and meet our criteria," that defeats the purpose of having a JAB and defeats the whole purpose of FedRAMP, frankly.

Mr. WILMER. Yes, sir. And what I will offer is, I've been in this job now for several months. Interestingly, most of the comments from the services mirror that of your constituents, of the companies, and the other cloud providers, in terms of wanting access to cloud capability faster.

I've seen very little resistance to accepting FedRAMP or JAB authorizations and much more interest, in terms of the folks that have come to our office, in trying to figure out how can we get this process more streamlined, faster, so that they can get capable to the warfighter at greater pace.

Mr. CONNOLLY. Mr. Meadows.

Mr. MEADOWS. Thank you, Mr. Chairman.

Mr. Wilmer, I want to followup on this, because, obviously, DOD is very good at checking the boxes and dotting i's, but sometimes what happens is—in your answer to the chairman, you said it's a core component. What we need to do is make sure it is the component. And there's a very different answer to that.

And I guess, if you will monitor that and make sure that we're not running into the future problem where they say, "Well, thank you, you've done everything that Mr. Wilmer suggests that you do, but here's this stack of other applications that you've got to fill out that are laborious."

You get our point?

Mr. WILMER. Yes, sir. I understand completely. And one of the things I'd like to emphasize in responding to that is that, of the 140 or so authorizations that we've provided, 120 of those required zero additional DOD work.

Mr. MEADOWS. Very good.

Mr. WILMER. So there are still—for, as you mentioned, sir, sensitive applications, capabilities like that, we do require some additional work to be done to address the increased threat posture for those applications. But the vast majority require no additional work.

Mr. MEADOWS. Thank you.

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

A final concern I've got, and I'm just going to throw it out there, but one of the things we've heard in the past as an excuse for why we have to sort of almost reinvent the wheel in application—we don't admit that, but that's what we're doing—is, well, wait a minute, I've got a separate requirement in terms of FISMA compliance, and I'm not going to put my agency at jeopardy to be FedRAMP-certified and risk FISMA compliance.

And maybe that's a legitimate concern, but sometimes we've been struck with the fact that maybe that's also an excuse to minimize risk and slow down this process.

And I'd just like any of you to comment on: Where are we on that issue, and how serious do you think it is as an impediment moving forward?

Mr. KLIMAVICZ. I'll take a shot at it.

In my five years in this job, I've not heard that as an impediment or anything like that. I mean, it's consistent with FISMA. And certainly within Department of Justice, we use all JAB ATOs. It's fantastic. I mean, the benefits are tremendous, in terms of speed and cost savings.

Mr. CONNOLLY. You're going to be the poster child for our bill. Thank you, Mr. Klimavicz.

Mr. Arrieta, did you want to comment?

Mr. ARRIETA. Yes. In the 50 days I've been on the job, I have not run into that issue.

And the FedRAMP folks from HHS that sit behind me, who do a fantastic job, are 100-percent focused on the use case and the need at HHS, and that is the first and most important question that we ask. We accept the JAB's authorization, and we look at the use case within HHS, and if there is a use care there, we accept it and move forward.

So we'll go back and talk with the cyber team and see if that's an issue.

Mr. CONNOLLY. Yes. Well, just keep us posted if you think it does crop up. If there's something we can do legislatively to provide that relief or clarify, we're happy to do it. If it's, in fact, no longer a problem, great. But we're going to count on you to give us some feedback.

And Mr. Cheriyan and Mr. Arrieta, being relatively new to your positions, I think bring a certain fresh perspective that we can all benefit from.

I want to thank this panel so much for your thoughtful legislation. I do want to say that there is going to be legislation in your future. We are determined to make sure that we address this by statute and that we codify it so it has a statutory anchor, which it does not have now.

We think FedRAMP is another one of the pieces of the IT legislation that we've championed over the years, always on a bipartisan basis. And we've been working with many of your agencies. We'd be glad to hear any concerns you've got.

We've be working extensively, for months, with the private sector as well, and we're going to hear now from four of them.

So thank you all for your willingness to share with us today. There may be additional questions submitted for the record

through the chair. We'll get them to you as expeditiously as possible and ask you to get back to us with answers as expeditiously as possible.

I thank you all. We look forward to working with you.

The first panel is now dismissed, and I would ask the second panel, as quickly as possible, to take their seats. We're not going to take a break.

Joining us for the second panel—while we're getting ready, I'll introduce them—are: Jonathan Berroya, who is the senior vice president and general counsel of the Internet Association; Douglas Barbin, who's the principal of Schellman & Company, LLC; Will Ackerly, who's the chief technology officer for Virtru; and Lynn Martin, who's the vice president of government, education, and healthcare at VMWare.

I would ask all four of you if you would be willing stand to be sworn in, and raise your right hand.

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

Thank you. You may be seated.

Let the record show that our four witnesses answered that question in the affirmative.

And, again, I'd ask you to limit your testimony to a five-minute-or-less summation. And if you'll turn on that button that says "Talk" when you're ready and speak into the microphone, so we can all hear you and pick you up on the record.

Mr. Barbin, why don't you go first.

STATEMENT OF DOUGLAS BARBIN, PRINCIPAL, SCHELLMAN & COMPANY, LLC

Mr. BARBIN. Yes. Good afternoon, and thank you, Mr. Chairman and respective members of this subcommittee, for the opportunity to share my testimony today.

My name is Doug Barbin. I'm a principal at Schellman & Company, where I'm responsible for leading the firm's FedRAMP practice, along with other cybersecurity assessment offerings.

Schellman & Company, or Schellman, is a top 100 CPA firm in the United States and distinguished from other large firms as we are solely and exclusively focused on cybersecurity compliance and certification services. Our clients range from startup firms to many publicly traded companies.

In 2012, Schellman became the first CPA firm to become a FedRAMP third-party assessment organization. Since that time, Schellman has grown to become the second-largest provider of FedRAMP assessments. And, in fact, FedRAMP has performed three times as many FedRAMP assessments as all other CPA firms on that list combined, including the Big Four.

I offer you my insights today as someone who has conducted more than 4,000 security assessments spanning virtually ever widely accepted technology compliance framework or program in the United States and many of those internationally.

The views I express in this testimony are on my own and should not be construed as reflecting any official position of Schellman.

So as a brief few opening remarks, as you know, the FedRAMP program was designed with the "audit once, leverage many" principle, with the goal of reducing the redundancies of Federal agencies each conducting their own assessments of vendors. It is my belief that this program has largely achieved those goals.

This leverage model is not new, and significant credit should be given to program leadership for their ability to launch and adapt the program in a timeframe that's significantly shorter than other similar compliance frameworks.

To add in perspective, the credit card industry has been doing this formally for 15 years. With the previous five years, when the credit card industry or the payment card industry was doing this, Visa and Mastercard were doing it themselves.

Based on my personal experience, I have just a few recommendations for the FedRAMP program as it moves forward.

First and foremost, protect the role of the assessor. We are the independent finder of fact, and we facilitate the conversation between the cloud provider and the authorizing body.

Some of the commercial compliance programs have blurred the lines between assessor, consultant, and decisionmaker. These roles are well-defined within the FedRAMP program and should continue to be strictly enforced. Independence between the parties should always be maintained in both fact and appearance.

Second, remember that the "R" in "FedRAMP" stands for "Risk." Some commercial compliance frameworks adopt a checklist approach to all-or-nothing compliance. Under these frameworks, achieving security is often secondary to achieving compliance with the letter of the written standard. This concern is even more critical due to the rapidly changing nature of the cloud technologies.

And I will say, as an aside, not in the written prepared testimony, I was very enthusiastic about the mention of a threat-based model, risk-based model for this program moving forward.

And then last but not least, community engagement. New guidance for requirements should be put out for feedback with reasonable timeframes for implementation. A more streamlined process for cloud providers to implement new products and services was mentioned as well.

And, in addition, from the last panel, I couldn't be more excited about the opportunity for automation. There are 300, 400, sometimes more controls that we have to manually comb through. There are vulnerability scans. Lots and lots of technical data. And the deliverables we're required to produce now were in Microsoft, Word, and Excel. So the opportunity for automation and to comb through that data is significant.

So I hope this feedback, along with the engaging dialog today, will assist the subcommittee in further moving the FedRAMP program forward in a positive manner. I thank you once again for the opportunity to share my views.

Mr. CONNOLLY. Thank you, Mr. Barbin.

Mr. Berroya?

STATEMENT OF JONATHAN BERROYA, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, INTERNET ASSOCIATION

Mr. BERROYA. Chairman Connolly, Ranking Member Meadows, and distinguished members of the committee, thank you for the opportunity to appear before you today to discuss the Federal Risk and Authorization Management Program.

My name is Jonathan Berroya, and I am the senior vice president and general counsel at Internet Association. Internet Association, or IA, represents over 40 of the world's leading internet companies. Our companies are global leaders in the drive to offer lower-cost, more secure, scalable, and innovative cloud services to customers in both the private and public sectors.

Cloud computing enables on-demand access to shared computing resources, providing critical services more quickly and at a lower cost than having agencies manage such services themselves, allowing those agencies to focus more of their resources on their missions and less on maintaining infrastructure.

To begin with, I would like to thank Chairman Connolly, Ranking Member Meadows, the subcommittee leadership, and your staff members for your continued commitment to government IT modernization. Ensuring that FedRAMP continues to meet the needs of all entities involved in the government's procurement of cloud services is an important priority.

IA cloud vendors are committed to the highest levels of information security and, collectively, invest hundreds of millions of dollars in compliance and certifications across both U.S.-based and international assessment frameworks.

Furthermore, our member companies have been engaged in working with the public sector for much of the past decade, many well before the creation of the FedRAMP Program Management Office or even the Cloud First Policy.

IA members support FedRAMP and efforts to facilitate the program's continued evolution. To that end, I would like to highlight four priorities that we believe will help ensure that FedRAMP continues to deliver value to all stakeholders, leading to greater adoption of commercial cloud services governmentwide.

First, we would like to see more reuse of authority-to-operate packages once a vendor has received FedRAMP Joint Authorization Board approval.

A core goal of FedRAMP's authorization process is to make the assessment of cloud offerings more efficient for vendors and agencies. The slogan "Do once, reuse many times," featured on the FedRAMP website, is a reference to the idea that once a service offering has been authorized for use, multiple agencies should be able to rely on that authorization to deploy that same service offering in their organizations.

In practice, however, there is a lack of reciprocity across Federal agencies that is due, at least in part, to the fact that each agency CIO must issue individual authorizations, which creates inefficiencies that undermine the central goal of the FedRAMP program.

Second, we'd like to ask that Congress establish the program in a way that will allow it to evolve over time. IA and its members support a FedRAMP process that is flexible and keeps pace with

innovation without imposing unnecessary bureaucratic requirements.

For example, it would be helpful to ensure that GSA and the FedRAMP Program Management Office have sufficient flexibility to fully automate the process of auditing the controls and missed baselines in the future, as this may result in a compliance workflow that requires fewer intermediaries, less paperwork, and faster processing.

Third, we ask that industry have a seat at the table to provide feedback on regular basis regarding the FedRAMP program.

IA members have noticed and appreciated GSA's demonstrated commitment to soliciting and acting on feedback offered thus far, including its creation of both the FedRAMP Ready designation and the low-impact SAAS baseline as a direct result of feedback from cloud service providers and agency cloud customers.

We feel that the creation of a formal industry advisory board or similar body would help foster ongoing FedRAMP engagement with industry, ensuring that this successful public-private partnership continues and that future policies are not created in a vacuum.

Fourth, we believe that this program needs more resources in order to assess and accredit the coming wave of cloud products. According to the GAO, the Federal Government invests approximately $90 billion in IT each year, with about 75 percent spent on operating and maintaining existing systems. Many of these systems will be modernized using cloud services, which means that dedicating adequate resources to fund the FedRAMP program will become even more essential to the cloud business ecosystem than ever before.

In conclusion, I would like to reiterate Internet Association's gratitude for being included in any legislative discussions regarding FedRAMP and for the opportunity to appear before you today.

We know that FedRAMP plays a critical role in the ongoing on adoption of innovative cloud services across the public sector, and Internet Association and its members stand ready to help the subcommittee succeed in its efforts to strengthen this important program.

Thank you, and I look forward to your questions.

Mr. CONNOLLY. Well done. Five seconds to go.

Mr. Ackerly?

STATEMENT OF WILL ACKERLY, CHIEF TECHNOLOGY OFFICER, VIRTRU

Mr. ACKERLY. Thank you very much, Chairman Connolly, Ranking Member Meadows, and distinguished members of the committee. Thank you for the opportunity to speak with you today about FedRAMP and our experience with the program as a tech startup.

My name is Will Ackerly. I'm the co-founder and CTO of Virtru, a small, D.C.-based software company that helps organizations and individuals protect their data wherever it travels.

Virtru successfully completed the FedRAMP process earlier this year. Security is core to our mission, so achieving FedRAMP approval was an important milestone for us. Based on our experience, I believe that the FedRAMP program makes an important con-

tribution not only to the security of our government but also benefits all other customers as well.

While deeply valuable, the process is long, time-consuming, and expensive. It is a process that can and should be improved. For large corporations, the effort required may not be a major obstacle, but for startups and companies like Virtru, the current process is daunting. Many startups may be not able to afford to secure FedRAMP authorization as it exists today.

Because the Federal Government can benefit from many of the innovations that young companies can provide, it is worth the effort to make FedRAMP authorization processes more accessible to smaller businesses.

In our case, the FCC wanted to use Virtru's data protection, and they were willing to sponsor us through an agency FedRAMP authorization. We officially entered the process in June 2017. We did not receive our final authorization until this past March, 20 months later. For startups like us, this is a very long timeline. More importantly, perhaps, it was unclear to us how long this was likely to take.

A related challenge was also the cost. Cost is a major consideration for startups, and at roughly $1.6 million in total costs, was a significant percentage of our annual revenue that had to be balanced against other priorities like hiring and further product development. As a privacy and security company, we were able to justify this decision, but when combined with unknown timelines, it can be a high-risk decision for most small companies.

Our challenge did not end with the authorization. The FedRAMP process also requires significant resources to maintain the authorization. This was not well-understood by us upfront. Many organizations may think that FedRAMP is a one-time effort, but, in our experience, the continuous monitoring requirements do entail a significant ongoing effort and cost.

We also found that the level of support and expertise available to help successfully complete the FedRAMP process varied significantly between different government agencies. This required us to adjust our engagement strategies for each specific agency.

In short, there were a few instances where the difficulties we encountered could be addressed by changes to the FedRAMP process.

Mr. Chairman, based on our recent experience with the FedRAMP process, I ask that the committee consider a number of specific recommendations, which I have described in my written testimony. I would like to provide you two quick examples.

First, streamline the process and costs by further empowering the PMO; to assist the PMO, the formal creation of FedRAMP leads at each agency as a force multiplier. This could help educate and shepherd companies and their agencies through the authorization and continuous monitoring process. This could improve the experience and the effectiveness and the cost for companies and agency personnel navigating this process.

Second, continue to empower agency sponsorship into the FedRAMP as an alternative to the JAB. Agencies best understand their own missions and are in the best position to identify and vet applicable solutions. While the JAB plays an important role, it would've been harder to justify the expense without interest from

a sponsoring agency giving us a roadmap to potential return on investment.

I appreciate the opportunity to address the committee today. I will gladly answer any questions you have. And I'm happy to make anyone at Virtru available for followup.

Mr. CONNOLLY. Thank you very much, Mr. Ackerly, and thank you for sharing your experience.

Ms. Martin?

STATEMENT OF LYNN MARTIN, VICE PRESIDENT OF government, EDUCATION, AND HEALTHCARE, VMWARE

Ms. MARTIN. Chairman Connolly, Ranking Member Meadows, and members of the subcommittee, thank you so much for the opportunity to speak to you this afternoon.

My name is Lynn Martin, and I am the vice president of our government, education, and healthcare verticals in the Americas at VMWare. I appreciate the opportunity to share our perspective on this important legislation and to relate our experience in taking our solutions through the FedRAMP process, as well as discuss some recommendations.

My experience dates back to the formation of the FedRAMP office back when I worked at HP. Since joining VMWare, I have also taken two products through the process, and I'm in the process of our third service through the FedRAMP. In addition, I'm working with our teams around other opportunities to funnel through there in joint partnership with both the JAB and the FedRAMP PMO.

Based on my experiences, I can personally say the FedRAMP process has taken great strides to achieve higher capacity and a more streamlined process since 2011. I would like to commend their efforts in making improvements.

Our collaboration and partnership with GSA has improved through each of the different authorizations I've been involved in. For example, in the last one over the past 18 months, the PMO has gone to great lengths to ensure that we understand and have more transparency than previously. There also has been engagement at our corporate site to ensure that we understand the process.

I commend Chairman Connolly on his efforts to support GSA on its ongoing efforts to improve FedRAMP.

VMWare believes that one of the most elements of the bill is that it formally provides a funding mechanism for the GSA FedRAMP Program Office. Dedicated funding will be a starting point to ensure that more FedRAMP authority-to-operate packages are completed in a faster manner.

The bill introduces much-needed clarity around the roles and responsibilities for each organization that has a hand in executing vendors through the process. Speaking from VMWare's firsthand experience in our recent interactions, we had to determine on our own which organization had ownership of what and interact with the office through organic understanding.

The clarity introduced in the bill would allow all vendors, not just VMWare, to build a repeatable plan, assessing our business case and returns, targeting the proper stakeholders on how best to navigate with the PMO. I believe this one step would cut down the

time that vendors go through because of the learning process on our end.

As we heard earlier, GSA has put some prioritization around the authorization. I think through the discussion earlier, one of the areas that I think there is an opportunity for improvement would be around looking at the agency ATOs, assessing the commonality of the security protocols, finding which ones are more commonly being used, and assessing whether there's a way to start with a baseline against those authorizations, and then resolve across the different agencies the percentage that maybe are outliers. So basically, if you look at the large number of protocols required for a JAB, there's a subset in the agency ATOs.

VMWare also agrees with the adoption for consistent metrics surrounding cost, quality, and time. The ability to drive measurements of the PMO will allow for not just accountability through the OMB but also transparency into the capacity of the PMO's ability to ATO public cloud services for the government to embrace quicker.

The final area that we would like to call attention to is the creation of Federal Secure Cloud Advisory Committee. We believe that the industry collaboration and coordination with the FedRAMP office is a key component of success. This will allow industry to interject best practices and allow GSA to stay ahead of the coming technology trends.

FedRAMP has become synonymous with Federal cloud security. However, in order for supply to keep up with demand, the Federal PMO must be given adequate resources so that the government can move further and faster in its modernization efforts.

VMWare is proud to partner with the government on its journey, and we look forward to further collaboration as the Federal Government refines and improves the FedRAMP process and we continue to bring to market innovation solutions.

Thank you for the opportunity to testify this afternoon, and I'm happy to answer any questions the subcommittee may have.

Mr. CONNOLLY. Thank you so much. And your praise of our draft bill, you also should be promoted and given a big, fat raise.

The chair recognizes the distinguished ranking member.

Mr. MEADOWS. Thank you, Mr. Chairman.

Thank all of you for your testimony. Obviously, it's a second panel on really establishing the foundation for legislation to move forward. The chairman, in his leadership, takes not just your testimony here but your written testimony, as well as some of the input, to make sure that the bill that we work on is perfected.

And under new House majority rules, these hearings are a prerequisite for moving any legislation. So you're playing a valuable part of making sure that not only your expertise gets folded into the bill that Chairman Connolly and I are working on but, more importantly, that your concerns get addressed.

You know, Ms. Martin, when you were talking about your testimony, the chairman is leaning over and he says, well, that's why we put this in and that's why we put that in. And so I want to let you know that you're being heard.

Mr. Ackerly, you talked about some of the obstacles for a small business—the uncertain nature of getting the approval and how

long and then how do you keep the certification up. How can we improve that?

I mean, because now you've gone through it, but unless somebody sees this hearing and they happen to call you and say, "By the way, I'm a small business; how long will it take me?", it's problematic. So how do we address those expectations and maybe draw down on how long it takes?

Mr. ACKERLY. Yes. Thank you for the question.

One of the biggest benefits we had were a few internal advocates within agencies that understood the value of our product, who were willing to engage with us and educate us——

Mr. MEADOWS. So had you not had that, you may still be waiting.

Mr. ACKERLY. Yes, we may not have been able to make the business decision to move forward.

Mr. MEADOWS. So you had to find somebody within the agency to basically say they see the merits of your product and they're willing to be an advocate for you.

Mr. ACKERLY. That's right. And I think, like, Department of the Interior was engaging with us early on, and we were immature in our understanding of FedRAMP at that point. They had been through some sponsorships, and they were willing to make that investment. They saw the broader value, which was fantastic. And same with FCC.

But I think, you know, being able to grow on that per-agency representation and have those folks educated and having consistency across agencies I think would be really valuable.

Mr. MEADOWS. So Mr. Berroya, you represent, for a large part, those that would dwarf the size of Mr. Ackerly's company. Is that correct?

Mr. BERROYA. Ranking Member, we have large and small members, but some would, yes.

Mr. MEADOWS. And so here is the concern I have. And it's proper that the two of you sit next to each other, in that you have behemoths that are—you know, they can work through it. And Mr. Barbin talked about, you know, being able to process and look at security things for thousands of stakeholders.

To put it in a different term, it's kind of like working through the FDA for a drug approval. Big Pharma, they understand how to do that. A small, little, startup generic company has a tougher spot with that. And it really is a chilling effect on new innovation.

So how do we work to make sure that some of your clients that are big and understand the process and some of the new folks that may come on the front, like Mr. Ackerly—how do we make sure that both of them understand what is required and how to navigate the bureaucracy?

Mr. BERROYA. Is that a question to me?

Mr. MEADOWS. Yes. It's a hard one, so I'm going to let you take it.

Mr. BERROYA. I appreciate that. I'll do my best to give you a helpful answer.

So for our small members—and, obviously, every company is going to be in a different position, and their experience is going to be somewhat different.

I've been advised that, for many of our small members, there's an argument that there's a market advantage. If you can make it through the process once, you're in, and you have that badge of having been certified, having been authorized, and that's something that you can use as a competitive advantage in other contexts when you're trying to woo additional customers.

But to get more directly to the question that you asked, I think the creation of a formal industry body to provide regular feedback about the FedRAMP process and how things are working that includes a mix of different types of companies, which is something that was alluded to on the first panel as well, would be something that would go a long way to ensuring that throughout the process the voices of both large and small companies are taken into consideration.

Mr. MEADOWS. All right. Well, thank you.

And I'll close with this, with your indulgence, Mr. Chairman.

Here is what I would like to see. In that body that actually is really the difference—one of the differences in the bill that we worked on last Congress is that stakeholder involvement and that advisory panel. Would it be helpful if—at the IRS, we have what we call a taxpayer advocate, or an advocacy. So if they run into a problem with the IRS, they have a group that they can go to and say, okay, here's where you go to, here's where you go to. Would something like that on FedRAMP be helpful to the process?

Ms. Martin?

Ms. MARTIN. Absolutely. I mean, like I said, even going through it four times, it changes. And they've made improvements, and we still took a long time. We started last July. We're not through yet.

Mr. MEADOWS. Yes.

Mr. Ackerly?

Mr. ACKERLY. Yes, I would support that. I think that would be fantastic.

I think, you know, per previous mention as well, you know, metrics for transparency and understanding, that is valuable as well.

Mr. MEADOWS. Mr. Berroya, does that help with some of what you were addressing?

Mr. BERROYA. I would have to get back to you because I represent a lot of members and I would want to make sure I had a clear feedback from all of them, but my——

Mr. MEADOWS. You want to make sure we don't mess up.

Mr. BERROYA. Exactly.

Mr. MEADOWS. Yes.

Mr. BERROYA [continuing]. my instinct on this one is it is likely helpful, yes.

Mr. MEADOWS. All right. Speaking for yourself, your instinct is right.

Mr. Barbin?

Mr. BARBIN. Yes. In short, yes. I mean, in many cases, especially some of the smaller companies that we've worked with, their biggest challenge has been the right person within an agency, what that agency needs to do to provide an authorization, and on an ongoing basis the continuous monitoring as well. So I think that advocacy group would be great.

Mr. MEADOWS. I think the chair's indulgence.

Mr. CONNOLLY. Absolutely. Thank you. Very helpful questioning.

So we're hearing—I mean, let us remember, FedRAMP originally, back in 2010, 2011, was intended to be an expeditious way of allowing entry into cloud services for the Federal Government, and it was supposed to cost maybe about a quarter of a million dollars and take about six months.

Now, Mr. Ackerly, you represent a startup—you're not even a small or medium-size; you're a startup—with apparently some expertise recognized or some capability recognized that was desirable, and it took you 20 months. And, by the way, at the beginning, no one could tell you, "Here is the timeline."

So you're betting that there will be light at the end of the day, or the tunnel, but it took 20 months and $1.6 million to be certified. Is that correct?

Mr. ACKERLY. Yes, that's right, sir.

Mr. CONNOLLY. And the other thing you did not anticipate was a recurring cost to maintain that certification. Is that correct?

Mr. ACKERLY. That's right.

Mr. CONNOLLY. Do you want to put a dollar figure on what that might cost annually in your budget?

Mr. ACKERLY. I'd have to double-check, but I think it might be $150,000 to $200,000 in annual costs.

Mr. CONNOLLY. All right.

And let me just explore that with all of you for a minute. But, I mean, at one point, you can see why the government wants maintenance, right? Maybe you're a startup particularly, you know, and it goes to hell in a handbasket. Or maybe your startup gets purchased or acquired, or maybe you expand by acquiring others, and all of a sudden the company we contracted with is different. Maybe it has foreign ownership. I mean, there may be lots of concerns that lead us to want to monitor the vendors to the Federal Government. That's not unreasonable. But, on the other hand, what does it entail, from your point of view?

I didn't see you, Mr. Grothman. We'll come to you right away.

Mr. ACKERLY. Yes, it comes from a few different sources. I will say that I think, as you say, there are aspects of this which are hugely valuable and important. I think through automation and also transparency—I think the metrics reporting and being able to track over time to understand what those are and what they entail will really help rationalize a business decision.

Mr. CONNOLLY. One of your recommendations to us was a power agency authorization instead of the JAB.

Mr. ACKERLY. Correct.

Mr. CONNOLLY. Let me just say, I understand why you might say that, but we kind of also look at it from the other point of view, that too many companies have been subjected to dual certification. So "Yes, you're certified with JAB, but sorry, our window is different, and you're going to have to start the process all over again." Imagine doubling your costs.

And remember that many companies have multiple Federal agencies, right? So they may move from national security to IRS or Social Security on the domestic side. And going to multiple windows to be multiply certified could be very expensive and time-con-

suming and unpredictable—everything you experienced, only multiplied by a dozen.

So while we understand a power agency to do it without having to have JAB certification, on the other hand, we don't want unwittingly to create difficult circumstances for companies from getting certified.

Mr. ACKERLY. From my standpoint, I think some of the most valuable things I think worth preserving and amplifying are the agency advocacies, the people who are at the agencies that understand the value, and making sure that they're in a position at least to nominate or try to fast-track through some sort of standardized process.

So if there's risk that there's going to be a dual track, you know, finding an opportunity for there to be agency advocacy and shepherding and common level of understanding across the agencies and representatives at each.

Mr. CONNOLLY. Just remember that what you're advocating for in some ways is already occurring, right?

Mr. ACKERLY. Correct. And so——

Mr. CONNOLLY. So if the JAB processes 12 a year, the other agencies are processing, I think he said 130, 80, or something like that, a large number.

Mr. ACKERLY. Yes. And what I'm recommending is formalizing that.

Mr. CONNOLLY. Uh-huh.

I've got two more questions, and then I'm going to call on Mr. Grothman, who has joined us, from Wisconsin.

Ms. Martin, I brought up an example in the earlier panel about a software approval for a same software, different application, but the process required a parallel or different or separate certification. Does that ring a bell with you at all?

Ms. MARTIN. Yes.

Mr. CONNOLLY. Do you want to just expand real quickly?

Ms. MARTIN. So when you take a software platform to a different company, like, a partnership with one company—so VMWare's strategy is we provide a hybrid cloud architecture, work with IBM, Microsoft, Amazon, more to come—that software layer is the same software layer with each of those different cloud services. Each one takes a parallel path on its own.

So part of the FedRAMP process—and I think it gets into the agency and the JAB's as well—is any new services have to go through the process again.

Mr. CONNOLLY. Even though it's the same software.

Ms. MARTIN. It could be the same but a little bit different——

Mr. CONNOLLY. Applied differently, yes.

Ms. MARTIN [continuing]. and you start over. They don't take the baseline assessment and say, "Okay, since you added this." It should, in theory, speed it up, in theory, once you get one.

Mr. CONNOLLY. But that was not your experience.

Ms. MARTIN. It is not our experience.

Mr. CONNOLLY. Okay. And you heard that Mr. Cheriyan said he would be look at that——

Ms. MARTIN. Right.

Mr. CONNOLLY [continuing]. at GSA.

Mr. CONNOLLY. Okay.

Final question. Mr. Berroya, I think you've heard both Mr. Meadows and I assent to the wisdom of industry input in some fashion so that industry's voice is heard in providing guidance of the process. But you talked about lack of reciprocity. And maybe you were here when Ms. Norton actually asked about the problem of reciprocity.

And I want to give you the final word and—and, Mr. Barbin, if you want to as well—comment on, what do you mean? What is the problem still, from your point of view, in terms of lack of reciprocity?

Mr. BERROYA. Thank you for the question, Mr. Chairman, and for the opportunity to be the last word. I'll try to keep it short, given the time.

Essentially, the perspective of our members is that, while CIOs play a very important role and they need to be able to make the risk assessments that they need to make, the ideal would be for FedRAMP to establish a ceiling rather than a floor for authorization, such that, if an agency, for example, wanted to engage in a pilot program and operate in a way that goes below what the standard authorization would require for that limited period of time so they can assess a new service offering, that they would be able to do so. But for, perhaps, a fully fledged new service offering that they're going to implement on a longer-term basis, that if FedRAMP established a ceiling, that might be a helpful way to inject a little bit more efficiency into the process and encourage more reuse.

Mr. CONNOLLY. I invite you to work with our staff and take a look at the draft legislation to make sure that we are adequately addressing that issue.

Mr. BERROYA. We gratefully appreciate that. We will.

Mr. CONNOLLY. Thank you.

The chair recognizes the gentleman from Wisconsin, Mr. Grothman.

Mr. GROTHMAN. Sure.

This is for any one of the four of you.

FedRAMP's current reporting and documentation structures are often redundant and excessively time-consuming. Has this inefficiency adversely impacted your industry's ability to work with the program?

Any one of you.

Mr. BARBIN. I'll take that, sir, as the 3PAO auditor.

I would agree. In my opening statement, I commented on deliverables being Excel spreadsheets and Word documents, a lot of manual analysis of a significant amount of data. I believe there's a significant opportunity there. Automation was brought up, you know, in the previous panel as well. So I would agree with you and concur that that is definitely the case.

Mr. GROTHMAN. Okay.

Is there sufficient communication between the FedRAMP office and agencies to you regarding the authorization process?

Mr. BARBIN. There is certainly—so I'd say there's sufficient dialog and communication between ourselves, the independent assessors, and the PMO. Certainly there's open and—very open and on-

going dialog with respect to that manner. We've been, you know, privileged to provide additional guidance over the years and help make improvements in certain key areas.

You know, with the agencies, that's typically been more on the PMO side; it's been less us, as an assessor. Our primary interfaces are going to be the PMO and the cloud providers that we perform the audits for.

Mr. GROTHMAN. Okay.

Any of the others?

Do you have a comment?

Ms. MARTIN. I have one.

So when we've been going through a recent agency authorization, our dialog's been more with the PMO and the agency directly, U.S. Marshals. But in the case of the 3PAO, they haven't been involved in those. But we have had better collaboration and communication around the process than previous experiences there.

I do think the transparency and the documentation and the automation recommendations would improve things significantly as well.

Mr. GROTHMAN. Okay.

Mr. ACKERLY. Yes, I would say our communication with the 3PAO and the PMO office have been fantastic, and when it comes to agency, it's been a little less consistent. Sometimes it's been great, and sometimes we've been learning together. And so I think there might be areas for improvement there.

Mr. GROTHMAN. If the FedRAMP program were codified, do you feel that would provide more security to you guys as investors?

Mr. ACKERLY. I think there are aspects of the bill that would absolutely create much more certainty and would make the business decision a lot easier.

Mr. GROTHMAN. Okay.

I'll yield the remainder of my time.

Mr. CONNOLLY. I thank the gentleman.

And I would just add a final word to his question, which was a good one. I happen to believe, and I think Mr. Meadows does as well—I don't want to speak for him, but—right now, the problem is FedRAMP is potentially an orphan. It was created administratively. It can be, you know, eviscerated tomorrow morning.

And so codifying it gives you some predictability, gives Federal employees who work on the program, you know, an anchor to guide them, and allows us to have regular guidance as we do through FITARA.

And so lacking a statutory framework sometimes can be a boon, but it sometimes also, frankly, can have unintended negative consequences. And I think we can restore some predictability and oversight just by codification. The bill, of course, does more than that. And so that's certainly our goal.

I want to thank all of you for sharing your stories today. Very helpful. As the ranking member indicated, this is creating the record that will allow us to go back to our colleagues and talk about potential draft legislation.

Thank you so much for sharing your story.

All members, without objection, will have five legislative days to submit additional written questions, if any, for the witnesses, and

I would ask that you would get back to us with your answers as quickly as you possibly can.

Mr. CONNOLLY. Thank you.

The hearing is adjourned.

[Whereupon, at 12:57 p.m., the subcommittee was adjourned.]