S. Hrg. 117–581

ROUNDTABLE FEDRAMP REFORM: RECOMMENDATIONS TO REDUCE BURDEN, ENHANCE SECURITY, AND ADDRESS INEFFICIENCIES IN THE GOVERNMENT CLOUD AUTHORIZATION PROCESS

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 30, 2021

Available via the World Wide Web: http://www.govinfo.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
50–895 PDF WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada
ALEX PADILLA, California
JON OSSOFF, Georgia

ROB PORTMAN, Ohio
RON JOHNSON, Wisconsin
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*
ZACHARY I. SCHRAM, *Chief Counsel*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
LENA C. CHANG, *Director of Governmental Affairs*
MATTHEW T. CORNELIUS, *Senior Professional Staff Member*
PAMELA THIESSEN, *Minority Staff Director*
AMANDA N. NEELY, *Minority Director of Governmental Affairs*
SAMANTHA ONOFRY, *Minority Counsel*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

TUESDAY, NOVEMBER 30, 2021

ALPHABETICAL LIST OF WITNESSES

ROUNDTABLE FEDRAMP REFORM: RECOMMENDATIONS TO REDUCE BURDEN, ENHANCE SECURITY, AND ADDRESS INEFFICIENCIES IN THE GOVERNMENT CLOUD AUTHORIZATION PROCESS

TUESDAY, NOVEMBER 30, 2021

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:31 p.m., via Webex and in room 342, Dirksen Senate Office Building, Hon. Gary C. Peters, Chairman of the Committee, presiding.

Present: Senators Peters, Rosen, Ossoff, Portman, Scott, and Hawley.

OPENING STATEMENT OF CHAIRMAN PETERS[1]

Chairman PETERS. This roundtable will come to order.

Certainly I am pleased, and I know I speak for my committee Members at the Homeland Security and Governmental Affairs Committee (HSGAC), to have representatives from both the government and industry here to discuss the Federal Risk and Authorization Management Program (FedRAMP), as well as our Committee's bipartisan bill, S. 3099, which is the *Federal Secure Cloud Improvement and Jobs Act of 2021*. I want to thank each and every one of you for taking time to be with us here today to share your insights on how FedRAMP can help agencies adopt some innovative cloud technologies while also ensuring robust security for Federal data and information.

I especially appreciate Senators Hassan, Hawley, and Daines for co-sponsoring the bill that is before this Committee. It is similar to a version that passed the House and is already included in the House version of the *National Defense Authorization Act (NDAA)*. The bill that we have pending before this Committee is a comprehensive, consensus set of reforms to drive quicker, more secure commercial cloud capabilities in government, which will improve cybersecurity, empower agencies to deliver modern digital services to citizens, and expand American leadership in cloud technologies which is, of course, incredibly important.

I look forward to discussing these reforms with an excellent group of experts. Again, thank you for being here today.

[1] The prepared statement of Senator Peters appears in the Appendix on page 25.

I now recognize Ranking Member Portman for any opening comments.

OPENING STATEMENT OF SENATOR PORTMAN[1]

Senator PORTMAN. Great. Thank you, Mr. Chairman. I appreciate your being willing to hold this hearing today, and I appreciate the witnesses being here because we have some real expertise before us, which is important in this area because it is complicated.

As you know, Mr. Chairman, I am not on the bill because I think we need to make some changes to it to make it fit better what I see as the potential problems in the codifying of the current practice. And you know, this is very important because this is the conduit for kind of a standard approach to assessing the security issues regarding cloud services, and it is incredibly important we get this right. I thank you for giving us a chance to review it today.

Mr. Fisic, particularly, thank you for joining us all the way from Dublin, Ohio, from Ohio College Library Center (OCLC), my home State. We appreciate again all of you being here and providing your insights.

The FedRAMP's "do once, use many times" framework has a lot of benefits. Once you get that security clearance, in effect, the reuse of authorized cloud systems has helped the government avoid an estimated $716 million in costs. So that is a good thing.

The current program, however, has weaknesses in it, which I hope we will talk about today in some detail. Those weaknesses, I believe, have left it vulnerable to foreign-backed hackers targeting cloud systems. Now that would include China; it would include Russia. Right now we do not have sufficient safeguards in place to identify and prevent foreign interference in our cloud systems, and I believe that must change before we codify this program. I know a lot of people share that concern.

This is especially important in light of FedRAMP's emphasis on reuse and the program's influence that goes really well beyond the Federal Government. The States, as an example, and local government often procure FedRAMP-authorized products because the FedRAMP label is on it. The Good Housekeeping Seal is on it, implying that these products and services are secure.

Further, FedRAMP relies heavily on the security assessments performed by private sector, third-party assessment organizations (3PAO). Surprisingly, cloud service providers (CSP) are the ones who choose which 3PAO assessor will conduct the security assessment of their cloud system and pays for it. To me, that creates a potential conflict of interest, and we should talk about that openly today. We have some ideas. I know we have talked to the Majority about this, as to how we could address that issue.

Finally, despite best efforts to improve the program, FedRAMP still suffers from high costs, long timelines, and inconsistent review processes across the agencies. As a result, Federal agencies have fewer cloud service offerings (CSO) to choose from compared to their private sector counterparts, hindering agencies from procuring the best service for their needs. As of today, as an example,

[1] The prepared statement of Senator Portman appears in the Appendix on page 26.

there are roughly 240 FedRAMP-authorized providers compared to the thousands available in the private market.

I look forward to a productive conversation today and how it would address some of these inefficiencies and some of the burdens in the FedRAMP system and how to improve the security posture of the government's cloud-based systems.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman.

I am going to introduce each of our guests one at a time. If you could take a couple minutes, introduce yourself and any thoughts that you may have, but try to be brief. We are not going to have the timer on, but try to just do it in a couple minutes because we want to get to some questions and have more dialog.

We are going to first hear from Ashley Mahan, Acting Assistant Commissioner of the Technology Transformation Services (TTS) at the General Services Administration (GSA).

Welcome.

TESTIMONY OF ASHLEY MAHAN,[1] ACTING ASSISTANT COMMISSIONER, TECHNOLOGY TRANSFORMATION SERVICES, GENERAL SERVICES ADMINISTRATION

Ms. MAHAN. Thank you. Good afternoon, Chairman Peters, Ranking Member Portman, and distinguished Members of the Committee. I thank you for the opportunity to participate in this roundtable today alongside my colleague, David Shive, the Chief Information Officer (CIO) of GSA and a member of the Joint Authorization Board (JAB).

I am Ashley Mahan, the Acting Assistant Commissioner of the Technology Transformation Services, Office of Solutions within the General Services Administration. I have spent most of my career dedicated to cybersecurity and mitigating risks to the security of Federal data. I have worn several hats, from writing System Security Plans (SSP), preparing for security audits, and serving as an Agency Information Systems Security Manager (ISSM) to leading FedRAMP.

I have also had a chance to work with the many different types of professionals involved in the end-to-end process, from cloud architects, incident responders, auditors and engineers to acquisition specialists and c-suite executives. They are always top of mind when we define improvements and develop the strategy for FedRAMP.

The program's success is largely based on our partnerships. We have listened to our partners, and they have been instrumental in how we have evolved and run the program today. We are about to celebrate our 10-year anniversary of FedRAMP, and along the way we have made steady growth and the pace at which companies get products FedRAMP-authorized has improved. In the last three years, we have more than doubled the number of authorizations from 100 to 240 as well as more than tripled the number of reuses of FedRAMP-authorized cloud products. The program's growth has even greater urgency given the continued demand for secure cloud technology and the need to work remotely.

[1] The prepared statement of Ms. Mahan appears in the Appendix on page 28.

As I look ahead to the future of FedRAMP, automation and modernizing our processes will be the focus of the program strategy. Meaningful and lasting change will only happen with continued collaboration with our government and industry partners. We will continue to leverage the insights of the cybersecurity community in order to solicit feedback as we continue to implement automation and modernize FedRAMP.

Our work is never done in this dynamic space. FedRAMP is committed to continuous improvement and transparency, driving the need to cultivate strong working relationships across industry and the Federal Government community in support of securing cloud technology. Thank you.

Chairman PETERS. Thank you.

Next we are going to hear from David Shive, Chief Information Officer at the General Services Administration and a member of the FedRAMP Joint Authorization Board.

Welcome.

TESTIMONY OF DAVID SHIVE,[1] CHIEF INFORMATION OFFICER, GENERAL SERVICES ADMINISTRATION

Mr. SHIVE. Thank you. I may need to speak loudly. It seems this is not working.

Chairman Peters, Ranking Member Portman, and Members of the Committee. My name is David Shive, and I am the Chief Information Officer at the General Services Administration as well as one of three Joint Authorization Board members for FedRAMP. It is an honor to be here today and a privilege to work alongside my colleague, Ashley Mahan, to discuss the FedRAMP program. I welcome the opportunity to share my organization's experiences related to FedRAMP as well as my experience as a JAB member.

The mission of GSA is to deliver the best value in real estate acquisition and technology services to government and to the American people. Our priorities are to deliver better value and savings, serve our partners, expand opportunities for small business, and make government more sustainable and be a leader in innovation. In support of that and as it relates to the Committee's objectives today, one of my organization's key goals in supporting GSA's mission is to deliver technology that provides a secure environment for doing business while ensuring that both information technology (IT) and business continue to run efficiently.

My role as a Joint Authorization Board member, along with the Department of Defense (DOD) and the Department of Homeland Security (DHS) CIOs, signoff of provisional authorizations to operate (P–ATO) based on FedRAMP packages provided by cloud service providers, assessed by FedRAMP third-party assessment organizations, and reviewed and validated by FedRAMP JAB technical representatives from GSA, DHS, and DOD. Separately, my organization with GSA, GSAIT, facilitates FedRAMP agency authorizations for cloud service provider offerings where GSA has a business need.

These roles allow me to have an intimate knowledge of, and experience with, the FedRAMP program, and I look forward to shar-

[1] The prepared statement of Mr. Shive appears in the Appendix on page 30.

ing my insights with you today. Thank you for allowing me the opportunity to contribute to this important topic.

Chairman PETERS. Thank you.

Next we are going to hear from Eric Mill, Senior Advisor to the Federal Chief Information Officer at the Office of Management and Budget (OMB).

Welcome.

TESTIMONY OF ERIC MILL, SENIOR ADVISOR TO THE FEDERAL CHIEF INFORMATION OFFICER, OFFICE OF MANAGEMENT AND BUDGET

Mr. MILL. Thank you. Chairman Peters, Ranking Member Portman, other distinguished Members of the Committee, good afternoon. Thank you for the opportunity to speak with you today about the FedRAMP program.

My name is Eric Mill. I serve in the Biden-Harris administration at the Office of Management and Budget as a Senior Advisor to the Federal Chief Information Officer, Clare Martorana. I work closely with her as well as with the Federal Chief Information Security Officer, Chris DeRusha, to accelerate the modernization of Federal technology and cybersecurity.

I have also in the past been a civil servant with the General Services Administration under two previous administrations as a member of the senior leadership team for the Technology Transformation Services. While I was there, I coordinated closely with the GSA CIO to authorize modern cloud tools for use in GSA. I was also the authorizing official (AO) at GSA for a large government-wide service that was working toward the FedRAMP authorization. In my engineering days, I personally built and deployed a few small government services to the cloud myself.

This administration recognizes the value and potential of the FedRAMP program to bring the best of the commercial cloud into government and to meaningfully raise the bar for Federal cybersecurity in the modern era and just to generally save time and money for both the government and for the private sector. We are relying on FedRAMP to help implement the President's Executive Order (EO) on cybersecurity, to support agencies as they migrate to a Zero Trust architecture, and generally to accelerate the adoption of modern cloud tools that improve agency efficiency and, ultimately, the public's experience with their government.

OMB is committed to continuing to work with you and Congress on legislation to bolster the FedRAMP program. We have been providing feedback to the Senate Homeland Security and Governmental Affairs Committee throughout the year to strengthen the proposed legislation based on OMB's and GSA's experience with the program and this administration's vision for Federal cybersecurity.

Thank you again for the opportunity to speak with you this afternoon. I am looking forward to the discussion.

Chairman PETERS. Thank you.

Next we will hear from Anthony Fisic, Executive Director for Global Security Services at OCLC.

Welcome.

TESTIMONY OF ANTHONY FISIC, EXECUTIVE DIRECTOR FOR GLOBAL SECURITY SERVICES, OCLC

Mr. FISIC. Thank you, Senator Peters, Ranking Member Portman. I am really happy to be here today.

As you mentioned, I am Anthony Fisic, Executive Director for Global Security at OCLC, and I have tremendous experience as a retired military officer working within a Federal environment, in the private public sector, in the global Software as a Service (SaaS) organization, working global compliance frameworks. We have great experience working with FedRAMP, been working with FedRAMP since 2017, and we currently are credited as a FedRAMP-authorized agency. I hope to share some of that insight with the team.

We are a global not-for-profit serving the library services community, and there are particular challenges that we face that many larger organizations may not face. I am happy to work with you guys today to discuss some of that. Thank you.

Chairman PETERS. Great. Thank you.

Next we will hear from Steve Kovac, who is Chief Compliance Officer and Head of Global Government Affairs at Zscaler.

TESTIMONY OF STEVE KOVAC,[1] CHIEF COMPLIANCE OFFICER AND HEAD OF GLOBAL GOVERNMENT AFFAIRS, ZSCALER

Mr. KOVAC. Thank you, Chairman Peters and Ranking Member Portman and the Committee, for holding this roundtable on FedRAMP reform. An honor to be with these wonderful people around the table, many I have known for many years, and I look forward to this roundtable to be very open and interactive.

As you said, my name is Stephen Kovac. I am the Chief Compliance Officer at Zscaler. I am here because I have a long history with FedRAMP and firsthand experience with the importance of FedRAMP to helping the Federal Government secure its systems as well as their networks and the challenges the programs have faced.

I have been involved with FedRAMP since the beginning. In fact, I was involved in FedRAMP before it was FedRAMP and when it was the blanket purchase agreement. I think back in those days it was the second one to be approved under the VPA. Since then, I have taken multiple systems through FedRAMP, both very small systems for moderate agencies to very large systems, at the HyperScope to JAB high, and multiple in between.

I have the knowledge of what many of the things you spoke of, Chairman and Ranking Member Portman, Senator Portman, in your opening statements, and I look forward to addressing those with you.

A little about Zscaler. We are very much like FedRAMP. We were born and bred in the cloud. FedRAMP was built for the cloud. We have the same mission, which is to make cloud safe for everybody, our company, as FedRAMP does for the government. We believe heavily in the FedRAMP program, and Zscaler's whole mission is around securing cloud and finding the best ways to do it and adapt as adaptions are needed.

[1] The prepared statement of Mr. Kovac appears in the Appendix on page 33.

To give you an example of what we do today, we run what we call our Zero Trust Exchange, which is built with two FedRAMP platforms underneath it, which is the base infrastructure to support 200 billion transactions a day run across our platforms. Our platforms are both high and moderate, and by the end of 2022 we will have two high JABs and two moderate agencies for our platforms.

We also have IL5 for one of our platforms, and we are IL5-in-process on our other platforms. Our goal will be to have IL5 by the end of 2022 as well across our platforms.

A little bit more about how Zscaler feels and myself feel. We obviously support S. 3099. We believe it is a very important legislation to move forward, and we believe that it is critical for the program itself and it will drive continuous improvements to the program while helping ensure Federal agencies have access to cybersecurity tools needed to protect them from today's ever evolving cyberthreats.

I assure you we, on a daily basis, correct over 200,000 updates for new cyberattacks that we find around the globe. So that gives you an idea of the scope of what is out there attacking us and why FedRAMP is so important.

It is also very important that we talk about the reciprocity with FedRAMP and the reuse, I mean, today. I am sure actually Dave will be talking about this. But you know, we talked about 241 agencies, but there is over 2,041 reuses of FedRAMP. So reciprocity is being done, and we do it today.

Reciprocity should be viewed in two ways. No. 1 is agencies' reciprocity of our FedRAMP platforms, but there is also reciprocities to the CSPs. Our CSPs are using our products to get their FedRAMP. This reciprocity creates a very good economy of scale to address cost issues when you can buy prepackaged services, which we will talk about later on today.

The "serve once, use many" is critical, and I think reciprocity is going to go for FedRAMP, but FedRAMP reciprocity is now extended to StateRAMP, which is the new program launched, I am sure you all are aware, as well as reciprocity is being heavily discussed with the CMMC program.

Like I said, we will address costs later, but one thing let me just say. When you consider FedRAMP and its time and cost, I ask that we take time today to look at, policy versus fact, experience versus inexperience, and really get down to the meat of why these sometimes take so long and why sometimes they are expensive and what part of that is on the CSP and what part of that is on the program. I think there is improvement in both areas, but there has definitely been drastic improvement since I have been a part of this program for over 10 years.

I am honored to be here and participate in today's roundtable, and I will help any way I can. Thank you.

Chairman PETERS. Thank you.

Next we are going to hear from Ross Nodurft, Executive Director at the Alliance for Digital Innovation (ADI).

TESTIMONY OF ROSS NODURFT,[1] EXECUTIVE DIRECTOR, ALLIANCE FOR DIGITAL INNOVATION

Mr. NODURFT. Thank you, Chairman Peters and Ranking Member Portman and the Members of the Committee, for holding this roundtable on FedRAMP reform.

My name is Ross Nodurft. I am the Executive Director for the Alliance for Digital Innovation. It is a coalition of innovative commercial companies whose mission it is to bring IT modernization and emerging technologies into government. ADI engages with policymakers and thought leaders to break down bureaucratic, institutional, and cultural barriers to change and enable government to access modern technology that can truly empower digital government.

ADI focuses on four key areas in our advocacy efforts: accelerating technology modernization in government; enabling acquisition policies that facilitate greater access to, and use of, innovation technologies; promoting cybersecurity initiatives to better protect the public and private sectors; and improving the Federal Government's technology workforce. Each of these areas must work closely with each other to allow for government mission owners and technology providers to partner with industry to build a modern digital government.

ADI's members include some of the leading technology and professional service providers in the public sector today, many of which have gone through the FedRAMP accreditation process or are working to achieve FedRAMP accreditation right now. These technologies underpin the Federal Government's modernization efforts and provide the backbone for many agencies' Zero Trust architectures.

Given our areas of focus, ADI applauds the work that Congress, the Members of this Committee have done to evaluate and craft legislation that can accelerate some of the changes needed to enable secure access to modern, emerging technologies. S. 3099, the *Federal Security Cloud Improvement and Jobs Act of 2022*, and its House companion, if enacted, would provide stability around the FedRAMP accreditation process and authorize resources needed to drive many of the reforms called for by the Government Accountability Office (GAO) and the Inspector General (IG) of the General Services Administration.

Over the last two years, ADI has expressed support for the codification of FedRAMP, and more specifically, ADI has stated and maintains its support for the authorization of additional and sustained resources to increase the number of FedRAMP authorizations, additional and meaningful collaboration with industry, the reuse and reciprocity of FedRAMP accreditations across the Federal Government, adoption of automation throughout the FedRAMP process, and creating market certainty through codification that gives innovative companies that are seeking access to the Federal market that assurance that they need.

I look forward to discussing these topics further and look forward to discussing it with my colleagues here. Thank you very much.

Chairman PETERS. Thank you.

[1] The prepared statement of Mr. Nodurft appears in the Appendix on page 35.

Our last participant is joining us via Webex, and that is Jeff Stern, Chief Executive Officer (CEO) of Chain Security.

TESTIMONY OF JEFF STERN,[1] CHIEF EXECUTIVE OFFICER, CHAIN SECURITY

Mr. STERN. Thank you very much. Good afternoon. I am Jeff Stern. I am the CEO of Chain Security. I first want to thank Chairman Peters and Ranking Member Portman and the Committee for inviting me to participate in today's roundtable.

Chain Security is a Reston, Virginia-based consulting engineering firm, and we are engaged in two related areas of work. First is securing the supply chains of U.S. commercial high-tech companies, typically Silicon Valley companies, from interference by foreign parties. The second area of our work is related, and that is supporting the compliance of companies that are regulated by the Defense Counterintelligence and Security Agency (DCSA), or the Committee on Foreign Investment in the United States (CFIUS).

Our consulting practice is informed by the unique combination of skills and backgrounds of our team. Our technology team includes members who have deep commercial product development and delivery experience in Silicon Valley. The company includes team members who have recent and deep experience in U.S. Government security practices and policies. We have extensive government security experience from organizations such as the CFIUS office, DHS, the Federal Communications Commission (FCC), and the Federal Bureau of Investigation (FBI). We include team members with recent experience at DHS' Cybersecurity Infrastructure Security Agency (CISA).

Most of our CFIUS and DCSA-related work is focused on the development and implementation of national security mitigations that the U.S. Government has required of our clients. In addition to that work, I am personally engaged in the graybeard program at DOD as part of the CFIUS investigation team for foreign technology companies on behalf of DOD CFIUS office.

The FedRAMP supply chain security information we have provided, and in the past we have spoken to Ms. Mahan about some observations we have made in FedRAMP supply chain security, but that work was developed in 2019 and 2020. It is possible that since then GSA has implemented or addressed some of the observations we have made in the past.

I will tell you FedRAMP is very important to our company because for our private clients, who are mitigating national security risk, we intend to move them into FedRAMP services in order to comply with their various national security agreements. We consider FedRAMP absolutely essential to the success of our clients who have to comply with government rules and regulations. Thank you.

Chairman PETERS. Thank you. I am going to just open up with a couple of kind of foundational questions for the Committee here and then move to my colleagues to ask their questions.

The first question will be to our government witnesses. Ms. Mahan, I will start with you, and then Mr. Shive and then Mr.

[1] The prepared statement of Mr. Stern appears in the Appendix on page 44.

Mill. Can each of you just briefly describe your roles in administering the program and how you believe Congress can help mature and improve the implementation of FedRAMP cloud security and adoption goals? Ms. Mahan.

Ms. MAHAN. Hi. Thank you, Chairman, for that question. In terms of how can Congress help, I think with the pending legislation that we have reviewed there are several aspects to the program in terms of increase reuse, increase agency participation in the program, as well as being able to usher in more cloud products through the authorization process, to give agencies more technology to choose from.

Finally also, feedback is very important for the program. I am a big believer in listening to our customers and taking that feedback to drive meaningful change across the program. So having a formal feedback loop, if you will, to receive feedback regularly, early, and often from our industry partners as well as government agencies will really help drive the program to be more effective in the future. Thank you.

Chairman PETERS. All right, Mr. Shive.

Mr. SHIVE. Great. Thanks for the question. I have a formal role and an informal role supporting the FedRAMP program.

The formal role is I am one of the Joint Authorization Board members along with the DOD and DHS CIOs. Reporting to me is a team. I do not do all the work myself. There is a technical representative that is the primary GSA focus for assessing the technical components of packages that we are reviewing, the cybersecurity of the cloud service providers that are applying to the program. My CISO leads the team that does the evaluation of the packages and is filled with Federal employees and contract augmentation staff employees. I sit on top of that entire organization, the machine that is doing one-third of the assessment work on the packages.

Informally, I am the CIO of a Federal agency. I am a consumer of the product that FedRAMP produces, and I have input. Ms. Mahan said that she solicits the feedback from the stakeholders who are interested in the program, and I am one of those voices that is speaking to her and speaking with cloud service providers, looking for ways to optimize and make more efficient the overall FedRAMP program.

Chairman PETERS. Any suggestions for Congress, how we can improve implementation?

Mr. SHIVE. Yes. I am proud to be associated with the FedRAMP program in that over its 10-year lifespan they have constantly iterated and tried to be relevant, not only with cybersecurity risk at the time, but compliance and risk management of the time. The team has done a good job of growing and shifting with the emerging cybersecurity threat and with the needs of the cloud service providers.

What I would say is as you are crafting and thinking about legislation that you create time and space for the program to be able to do that, to continue to iterate over time, be less prescriptive, be more allowing, knowing that we cannot fully assess what the cybersecurity threat in the future is going to look like and that the team

needs to have that agility built in through any legislation that would be left.

Chairman PETERS. Very good. Same question to you, Mr. Mill.

Mr. MILL. Yes. The Office of Management and Budget has a number of roles with FedRAMP. The FedRAMP program itself is currently ultimately a creation of the Office of Management and Budget, and its authority comes from policy that OMB has set out.

The work being done on legislation to support FedRAMP would give the program quite a bit more certainty and stability, and so that is something that we are supportive and interested in continuing to work with you on. Our office oversees the development of cloud security and security policies generally in the Federal Government and is ultimately responsible for setting the tone as well.

One of the things that I think is really resonant with some of the other comments that you have heard here from industry and others today is really wanting to support a truly robust use of commercial cloud services, big and small, in the Federal Government. The Federal Government does not have to always be a late adopter, and sometimes it is more risky to be a late adopter, and the FedRAMP shows a lot of promise in being able to enable that.

So that is what I would answer for that.

Chairman PETERS. Mr. Kovac, your company has several products that have been FedRAMP-authorized, as you mentioned in your opening comments, as well as a variety of security levels. So that is pretty extensive experience that you have representing a cloud service provider in the Federal marketplace.

I am interested if you could discuss how this program has evolved over the years that you have been engaged in it and what additional changes you would like to see the GSA and OMB and other agencies make to reduce costs, to avoid duplication, and to enhance effective security in the process.

Mr. KOVAC. Thank you for the question, Chairman. It is a great question. Everybody learns over a period of 10 years, right? We are all going to get better. In the initial years, in the initial times, FedRAMP was onerous in many of the processes. It was getting its feet under itself, a lot of back and forth, not a lot of collaboration in the early years. It was you send your document in and your document came back. Security policy was changing, and it was changing in the middle of an authorization, and therefore, you would have one policy and all of a sudden you would have to go back and change it again.

What you have seen through a tremendous amount of work and effort from the FedRAMP office is really getting that process very automated, very collaborative, and I think it has allowed us to be much more nimble in how we approach a FedRAMP authorization.

You talk about many of them, I mean, I have done an authorization that took four years back in the early days. I bragged that obviously here that we have the record of two and half months for a FedRAMP JAB high. There is for a very large system. Obviously there is improvement. The improvement is there.

It has matured over the years, and I think it has matured by, No. 1, obviously the natural maturation of any process throughout the years, but I think also, they have been able to really learn from the more and more patches that have come through. They have

learned, what to look for, what are the things that can trip up an agency, what are the things that can trip up a CSP, what are the things that trip up an agency.

I assure you anybody that has ever sat down in a room and done a boundary discussion with the FedRAMP office you will learn that it is a very strict process. That process has gotten stricter over the years. It has not gotten easier, and yet, we have accelerated the number of FedRAMP authorizations. So something is working, right?

Yes, you talk about 241 authorizations equated out to 2,800 reuses comes out to something like 10 reuses by 77 agencies. If you equate that back to every one of those agencies having to do an Authorization to Operate (ATO) on their own without FedRAMP, we would be nowhere near where we are.

We have the Open Security Controls Assessment Language (OSCAL) now is coming out, which is automation of the SSP process. I think what you are seeing is just the natural growth and the market accepting and knowing how to get through the process.

There is a group of us that all work together, my peers in the industry, that we know how to do the process. Then there are the people that come through that just do not know how to do it. FedRAMP has made it much easier for them to get through it.

I blew all over the board with my answer, but I was trying to get across the fact that there is a lot of factors here, but the most important is the enhancements they have made to just the knowledge base and the collaboration. It is just phenomenal these days.

Chairman PETERS. That is great. I will have more questions, but I want to turn it over to Ranking Member Portman. I know he has a number of questions.

Senator PORTMAN. Great. Thank you, Mr. Chairman. I want to leave time for Mr. Hawley to also ask some questions before he has to take off because I know he is busy. I will be as brief as I can, but I have a lot of questions, as you know.

I am for codifying. I am for standardization. I am for more certainty and predictability going forward. I think it is a good idea. FedRAMP, in practice, I think is a good idea and, it is essential. Yet, the security issue just bothers me. I want to be sure we fully vet this. Foreign interference in particular is a deep concern of mine, and I think it is of others as well.

Second, I want to talk about potential conflicts of interest with the assessment process. I do not know why we have the companies that are getting assessed, choose their assessor and then pay for the assessor. It seems to me that creates at least an appearance of a conflict.

Then third is just the cost and timing issue. You have addressed that maybe things are getting better, but you know, we need to allow the service providers to be able to have a sense of how much time this is going to take and, like any regulatory process, how much it is going to cost to make sure that we are getting the very best cloud services. That is the whole idea here, right, is the Federal Government has the gold standard.

On the first issue, which is the foreign interference, this Committee has been very active on this issue. The Safeguarding American Innovation Act came out of this Committee. Senator Hawley

has been really taking the lead in this Congress to protect the government from data from China through legislation that would ban TikTok, as an example, on government devices. Other Senators have similarly been very involved, on both sides of the aisle. I know we care about it a lot, and this Committee tends to be a place where a lot of that happens.

My concern is that the source of some of this code that we are relying on in the Federal Government may well be from foreign entities and specifically engineers in China, and I just want to make sure I understand why we would want to permit that.

Then the second issue that I have identified is that we do not have to keep up with the disclosures. You make an initial disclosure saying I am owned by this company from the United Kingdom (U.K.), this company from the United States or whatever. But then, as an example, not to just focus on China, but if China becomes an owner, there is no requirement to update that disclosure, as I understand it. To me that seems like an obvious problem that ought to be addressed in this legislation. If we are going to codify this thing, let us be sure that we are not putting ourselves in that position.

Mr. Stern, turning to you, you are the one that is not here, so you are easy to turn to. Can you talk a little about that? Your observations on supply chain risk and foreign interference as it relates to FedRAMP.

Mr. STERN. Sure. Thank you, Senator Portman. I am going to talk about three things. The first is the system security plan and the fact that FedRAMP authorization of the SSP has not seemed to look or assess the providence of the software and the service offering. As you mentioned, the code could all be developed in China; yet, there is no disclosure requirements here.

Our recommendation around that has been that at least—you may not be able to stop this because the global supply chain, but at the very least, the buyer or user at DOD or at DHS or wherever should be able to know how much of the code was written overseas and what percentage was written overseas. We have offered up some metrics as recommendations in the past about how to sort of what I will call the truth in advertising or truth in disclosure, not only in the authorization process but also for the purchaser who is going to use the service.

The second is that the system security boundary for authorization seems to be defined too narrowly. We have seen cases where, for example, even though your customer care people are here in the United States, no one is looking at the customer care system itself and who is maintaining it and what engineers overseas, particularly in a country like China, can have access to the entire customer care information, including the personal identifiable information (PII), of U.S. Government users, the IP addresses, their e-mail addresses, their names, phone number, et cetera.

The third is we observed a case where one of the 3PAO organizations had already been through a CFIUS process where CFIUS and DCSA, as a result of a foreign acquisition of the company, required establishment of a mitigated subsidiary to hold a security clearance; yet, it was not the mitigated sub who continued to be the

3PAO. It was the foreign, unmitigated parent of the mitigated sub who continued as the PAO.

There is a thing called an SF–328. It is a form which declares how much foreign ownership you have. We believe every 3PAO has to fill out an SF–328 both at change of ownership but annually. New 328s, which are easy to fill out, should be filed by every 3PAO.

Senator PORTMAN. Great. Thank you. By the way, it was the PAOs that I was referring to in terms of that ownership requirement and having to update it, and it seems to me that is a relatively easy fix.

Mr. STERN. Very easy.

Senator PORTMAN. Maybe the first one is a little bit harder. We have recommended some language that just gives the GSA the authority, and the requirement really, to review "the sufficiency of underlying standards and requirements to identify and assess the providence of the software in cloud services and products in the FedRAMP program." So that would allow GSA to assist National Institute for Standards and Technology (NIST) in developing and improving the standards regarding foreign interference.

Ms. Mahan in particular, do you have concerns with that kind of language? Do you think that does that not go far enough, or does it go too far? What do you think about stopping this concern we have about foreign interference?

Ms. MAHAN. Thank you, Senator. I just wanted to thank Chain Security and Mr. Stern as we met, as he alluded to, in 2020, where he provided some of these recommendations. We had a good conversation discussing the recommendations he brought up today as well as we took the due diligence and steps to research those out. There were some things that we were working on already in progress and things that we implemented based on his recommendations and research.

I do think that this is an area that is continuing to evolve daily, and as from a program standpoint, we are committed to evolve with it. In terms of geolocation for the government's most sensitive, unclassified data, we call that part of our high workloads. There are geolocation restrictions to U.S. and territories with U.S. jurisdiction, as well as we are continuing to work with NIST and with future updates to provide additional security controls when it does come to supply chain.

But again, we are absolutely committed to be working with the Committee, as well as different government agencies and industry, to ensure that the program continues to evolve as these threats are continuing to evolve as well.

Senator PORTMAN. OK. I want to let my colleague, Mr. Hawley, jump in here, but let me just say—and we will get back into the potential conflict of interest issue I have and also the cost and timing and the compliance burdens. But with regard to this issue, I mean, from what you are saying, it sounds like you agree with Mr. Stern generally and you agree with a solution that gives you all not just the authority but the requirement to do that important compliance to make sure that we are not seeing foreign interference.

Ms. MAHAN. Absolutely. This is a critical area, a focus area, and we are committed to evolve and working with our industry and agency partners on this.

Senator PORTMAN. OK.

Ms. MAHAN. Yes.

Chairman PETERS. Before Senator Hawley, we are working on changing that language right now. I think these are very good, constructive concerns that you have raised that we are going to make sure is in the language going forward. Thank you.

Senator Hawley.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Yes, thank you, Mr. Chairman. I just want to follow up on this line of questioning. Just so that I understand, Ms. Mahan, you think that Senator Portman's—the language that he is talking about, you support that? You think that that would go some way toward addressing the software providence issue?

Ms. MAHAN. I would have to look at the specific language, but again, supply chain security is of utmost importance and concern at this time. I would be more than happy to take that particular language, continue providing technical assistance that we have done on prior versions of the pending legislation, and you know, provide any particular thoughts regarding the specific language.

Senator HAWLEY. Are there other measures, other reforms, other amendment language, frankly, that you or other Members who are here, other witnesses who are here, would suggest to get at this issue of software providence? I think Senator Portman has raised an important issue. I share his concerns.

I am just curious. Beyond what he has proposed in terms of allowing FedRAMP to work with NIST in developing standards, are there other measures that you or others might put forward for our consideration as we work on this legislation? Go ahead, Mr. Shive. You are sort of nodding. So the old professor in me will take that as you want to comment.

Mr. SHIVE. I think this goes back to one of my opening statements. There is a certain advantage in being less prescriptive in legislation. The risk changes. You look at the risk associated with cybersecurity. It has changed and morphed over time, and the program has changed and morphed right along with it. Mr. Kovac talked about how the way that things are done, that are assessed now, is more lightweight, easier, even though the overall risk profile has gotten profoundly more complex and does so every single day.

Supply chain is going to be the same exact way. The program has been able to, under current less prescriptive legislation, to be able to shift, change, morph, mature, and become stronger in that environment. We suspect that under the supply chain risk that that same less prescriptive model would be most effective because we cannot anticipate what that threat is going to look like in the future and we run the risk of tying our hands if we are too prescriptive.

Senator HAWLEY. Fair enough. Do others have thoughts? Yes, Mr. Kovac, go ahead.

Mr. KOVAC. Yes. Thank you, Senator. I look at this as an interesting question because if you look at the SA controls that currently exist in FedRAMP there is absolutely sufficient controls for any offshore development to know what is being done before you load it into your boundary. The controls we must meet, the testing we must do to that code disclose where that code has come from. These are all today part of the FedRAMP authorization process.

There is also the CISA directive on working with restricted countries, right? So immediately, when CISA came out with their leadership, the next day, within hours, we had 24 hours to respond back to FedRAMP that we were not doing business with these restricted countries.

This is an issue that is growing. But if we are to say we cannot develop software outside of the United States, let me assure you a lot of companies, including us, are going to have a lot of problems because some of the best work in the world is done in countries like India and other places that are partners of ours.

As long as these SA controls are followed there is honesty, and the 3PAOs are expected to do these, I fully believe they do, and we can have that discussion, Senator—I think that the SA controls today are sufficient.

I was working with a company where we built a FedRAMP moderate cloud, and we were going to sell it to BT Group. The first thing we had to do was contact the FedRAMP office, and we had to apply for permission to do that because they were foreign-owned. Obviously, they were BT United States, but they were a Foreign Ownership, Control or Influence (FOCI). Immediately, that came in, and we had meetings with them, discussion and full disclosure.

Unless it was done, unethically, I find it hard to believe that someone owning a FedRAMP cloud could just sell it off. But you know, things could happen. Today, there are proper controls, and as long as you have an ethical group, there is coverage there.

One last thing I did want to address on Mr. Stern's comments was around the boundaries. The boundaries is a very interesting discussion because I am a firm believer all U.S. citizen cloud data is anonymized.

When we build clouds, that go to the IL5 level, the IL6 level—we start with that plan. We go through moderate, high in other ways, but that is the plan. Many cloud planners do not do that, right? They are building just to moderate to meet their current market. But either way, there is still the idea of when you talk about support systems that is customer data. That is metadata. That is PII. If it has that, it is required to be in the boundary. That is a requirement of FedRAMP.

If there are companies that are not putting this data inside the boundary, then you know, we need to have language or a process to figure out why that is happening because the controls are there. You should not be able to do that.

If you want to extend this boundary and say everything should be in the boundary, you are not going to have a FedRAMP program because where does it stop, right? At what point do I have to put my HVAC system in the boundary that powers electric in my building. At some point you have to draw a line. And where you draw that line is metadata, PII, right? That is exactly the things we

spoke about. The government PII that, IP addresses, Social Security numbers, phone numbers. Two things that you could tie back to a person to create PII.

I think, yes, the boundary is very tight here and unless you are having a 3PAO that does not understand the boundary then you should not be able to have a control system with metadata outside the boundary. That is a requirement.

The last part was, just this summer we worked with FedRAMP—well, Zscaler did—because FedRAMP high we firmly believe should not be processed outside the United States. It is the most U.S. sovereign-owned or—I forget how we worded it. But to me, we are passionate about this. Moderate boundaries, I think that is up for an agency to decide. But when you are talking FedRAMP high, that is critical data that should be processed on U.S. soil. Again, that is a requirement of an SSP.

I think these things are there. Tightening language in the bill in any way we can I would support. But the good news is the foot—the benchmarks are there today.

Senator HAWLEY. You can go ahead.

Mr. NODURFT. Senator Hawley, thank you. First of all, thank you for your co-sponsorship of the bill. I think it is wonderful.

I do want to call out one particular thing is as you are looking at language, making sure that there is not divergent areas within government who are developing different ways of addressing this particular risk. In other words, we have things that are evolving in NIST right now from the cybersecurity EO around supply chain security risk. To have something come out that is a guidance or guidelines that agencies are then passing on to their IT technical providers and cloud service companies and then to turn and have FedRAMP have additional authority to do something else would be problematic for a lot of the companies. So making sure that those are aligned in whatever language we do is extremely important as well.

Senator HAWLEY. Very good. That is very helpful.

Thank you, Mr. Chairman.

Absolutely. Mr. Stern, do you have a view on this? Do we still have Mr. Stern? There we go.

Mr. Stern, do you have a view? Back to the question of in addition to what Senator—the language Senator Portman has proposed that we have been discussing, do you have a view on other affirmative steps that might be taken to address the software providence issue or the other related issues that we have just been talking about, from a security perspective?

Mr. STERN. Yes, Senator Hawley. Can you hear me?

Senator HAWLEY. Yes, I can.

Mr. STERN. Perfect. Thank you. Well, probably my view is that everything Senator Portman is talking about is language is important.

What I would add to it is something I mentioned just in my sort of almost introductory remarks, and that is that I believe the Federal user should know. It is not just the authorization at the FedRAMP level when something is authorized that we should be looking at providence, but we should be looking at providence and measures of providence and disclosing them as part of what I will

call consumer awareness to any Federal purchaser because a CIO, for example, at the Department of Education may have a different criteria and assessment of risk related to providence than a user in the intelligence community or at the Department of Defense.

I believe that what I will call disclosure is important to the end user, and it should not be behind a curtain that only the folks in the FedRAMP or governing FedRAMP should be involved in.

The second thing is I respect that Zscaler is passionate about authorization boundaries, but because we are in the supply chain security business we sometimes drive deeper into how things are built in companies. While I believe Zscaler is a great company doing stuff, we know that most of the stuff that is delivered in FedRAMP, almost everything that is delivered in FedRAMP is not built for the Federal Government. It is commercial products that are being adapted for the Federal Government.

I is very unusual, for example, in what is technically called third-level support for when there is a trouble ticket that has to go back to developers, if the developers are in a foreign country, it is very normal for there to be free text fields, for example, in the trouble ticket system that includes PII that a developer in a foreign country who has to fix the problem can see.

Those are the two things that we think are important, that really customer care systems need to get locked down and folks who are purchasers in the Federal Government should have exposure to some statement of providence and where the code is both developed and supported. That is my comment.

Senator HAWLEY. That is very helpful. Thank you.

Thank you, Mr. Chairman.

Senator PORTMAN. You are welcome. Yes, the other issue we talked about—and thank you for all that input. We have a little difference of opinion perhaps as to how the FedRAMP system currently works as it relates to inquiring into the origin of software or code in a cloud service offering, but that is a factual matter we just need to be sure we all understand.

I do think that this risk is only going to increase, as was said. To Mr. Shive's point, I do not think that is prescriptive language at all. In fact, it gives you the ability to be able to do what I would assume you would want to do anyway but make sure that it gets done.

In terms of potential conflicts of interest, looks like we are going to have some differences of opinion on this, too, and that is good. That is how we end up with legislation that actually makes sense. I just look at this, and I think, all of you respect your 3PAOs. This is for those who might be listening and are not following all the acronyms. That is the third-party assessment organization, and these are groups that do the assessment but at the behest of the company that is providing the cloud services. As I understand it, they pay for the service and they choose the 3PAO. Is that correct?

Now again, I am sure that the 3PAOs that you all work with are all respectable folks and so on, but that just seems like a potential conflict of interest to me. Isn't there a better way to do it so that you get an assessment that does not have that, to use the word "cloud" a little differently, that cloud in terms of what the conclusion is?

One idea I have had is rather than relying on private sector third parties who are paid for by the cloud service provider is to get a panel of experts—in this case, GSA, NIST would be involved—and have that panel of experts assess the security of the FedRAMP services.

The cost would not be borne by taxpayers. It would be borne by the user, which is the same company that was going to pay this company on the private side that they had chosen, that they are paying, to give them the answer. Instead, you would be using an entity which is independent, and there would be a user fee attached to it. There would not be an additional cost, but there would be a distance there, in other words, an assurance that this conflict of interest would not be present.

What do you all think about that? Is that a crazy idea? Is that something you thought about, and do you have other ideas? Let us start with you, Ms. Mahan.

Ms. MAHAN. Thank you. When we first established the program many years back, the 3PAO program, we mimicked it after how industry—like traditional certification programs that industry goes out and seeks today. We developed a framework using the ISO 17020 standards, which is an industry recognized standard. Within that standard, there is impartiality and independence clauses.

We have a robust monitoring program on FedRAMP that whenever we receive assessments from 3PAOs we provide feedback. There is performance escalation criteria as well to help support and to monitor 3PAO performance, especially when it comes to this area.

I appreciate your suggestion, Senator we are always receptive to feedback. We will take it into consideration, continue to work with the community as well as our stakeholders to drive change on the program.

I will say that the 3PAOs play an absolutely critical role within this FedRAMP ecosystem. They are charged with validating that the security implementations from cloud service providers are true and accurate, which gives agencies, in turn, the ability to make those risk-based decisions in terms of using those cloud systems.

We are absolutely on board to continue evolving this program, but just note that the way that we did establish it was also based on industry-recognized protocols that are in place today with other certification programs.

Senator PORTMAN. Mr. Kovac, do you have thoughts on this?

Mr. KOVAC. Senator, I would say Zscaler is a public company and we pay Pricewaterhouse to come do our audits, our financials. I do not see the difference. But I do not see a difference. I pay when I go to get my ISO, our global compliance, whether it is my GDPR for the E.U. or whether it is my IRAP in Australia or whether it is my ISO or my SOC 2 or my SOCs. I am always paying an independent auditor that I hired.

I think that the FedRAMP policy is in line with almost every other audit that we do across the corporate world. I think that you have to believe that your 3PAO is going to be ethical and do their job. If they do not, me as a CSP, would throw them out, and I have done it for sure.

I will tell you that to think that it stops at just the 3PAO, it does not because once we finish our 3PAO and we get our "they said OK" then it goes into the FedRAMP world, where they now do their, and as Ms. Mahan just said. They do their assessment of our 3PAO's work, and then the JAB does the work all over again. So they are heavily involved in this process.

I think that trying to find a way to regulate it to a group of people is going to slow the process tremendously, and like I said earlier, it is the way we do all our independent audits, and I would be troubled to get away from that.

Senator PORTMAN. Yes. I appreciate that. I make the obvious point that we have had some captured auditors as well.

Mr. KOVAC. Yes, I agree.

Senator PORTMAN. This is about security. It is not about auditing your books. It is about ensuring that we do not have the terrible situation that could occur, where you have a lack of security within the cloud services that the Federal Government and we taxpayers are all relying on. It is a different sort of assessment than, what Deloitte might do for your company in terms of an audit.

Any other thoughts? Mr. Stern, do you have any thoughts on that?

Mr. STERN. Yes, Senator Portman. Thanks for asking. First of all, I think the 3PAOs are absolutely necessary to have a scalable program, which means a program where you can bring services on and authorize services in a timely manner, on the one hand.

On the other hand, I think one potential approach here is to have the 3PAOs directly under the supervision and assigned by GSA so that GSA hires the 3PAO and assigns the 3PAO and where the company pays as part of some sort of fee to have it done, but the 3PAOs are hired and assigned by GSA. That may be the solution.

Senator PORTMAN. Yes, that is something that I think makes some sense, too, to look at because you could have a panel of various auditors in essence and instead of having the company choose the auditor it would be from a group of auditors that you all, being GSA, have certified. In essence, you are certifying them anyway, right?

Ms. MAHAN. That is correct.

Senator PORTMAN. Yes. So you could make the decision even on an arbitrary basis if necessary, which would cut out obviously that issue of you are choosing your own 3PAO auditor and paying that auditor. You would still pay, but you will be paying a fee. I think that is an interesting idea as well.

My final one is just on the cost and the timing and the compliance burdens, the consistency across agencies. What can be done to improve that? Mr. Fisic, I am going to ask you to address that.

Mr. FISIC. Thanks, Senator. For one moment, I would like to address, having the—can you hear me? Does that work? OK. Thank you.

Just one second, please. I would say that, having the GSA or the FedRAMP Program Management Office (PMO) select your 3PAO works against smaller organizations from a cost perspective, kind of leading to the next question here. We create efficiencies at scale, where I have 15 global certifications we maintain. If I use Schellman or Coalfire or these larger global organizations that are

well respected, No. 1 and two of FedRAMP authorizations, it really works against us as a smaller organization. Sure, we will get some benefits if GSA at scale for the government, engages them, but that is a concern there.

We are a FedRAMP-tailored low. We do not have a lot of PII. We have heard a lot of high, moderate supporting these large organizations. We support libraries, the Library of Congress, libraries on military installations as part of our core support to the Federal Government. As a library services company, we do not charge a lot of money as a not for profit.

Some of the concerns we have is I have two full-time governance analysts running. I have a full service now, which is a governance risk and compliance system running. I have 400 developers. We have 150 and up applications; 26 are in FedRAMP scope. But the churn created for smaller organizations, we spend up to $10 million a year as a not for profit that makes 200 a year on security and, trying to do the right thing to support our customers.

I think that as we talk about these highs, moderates, lows we really need to think the impacts to the smaller organizations and maybe an additional lens of risk.

I understand, 30, 90, 60 days to remediate any sort of vulnerability. That is a huge impact for a smaller organization. If there was just that additional risk assessment—say, OK, these guys, they know what book you took out, right? Why are they even in the program? Sure, it helps us. It is an easy framework. I can communicate to the board. I can do all these things. It is good practice and things we do anyway, but the sunk cost to do that really impacts our bottom line and serving the communities and some of the least represented people globally. It is not just in the United States, the communities we serve.

I would ask the Committee to look at that. Think about that additional lens, a true risk picture outside of these mandatory high levels, moderates or lows. Let us put some reality check in there. We are smart enough where we can just, look at an organization and formalize that, just an additional check or an outside agency look, to say: OK. OCLC or another smaller company, you do not really have a lot of data that the Federal Government is concerned about. Maybe we can lower that risk level, lower the costs, some of those reporting compliance requirements, monthly reporting, going through the churn of POAMs and all these other things.

I am a fan of FedRAMP. I have been with the program for 4 years. It has continually evolved and gotten better. I think it is the right thing for the government to do, as somebody who worked for the DOD before, and I fully support it.

But I just ask for the team to look at it through that additional risk lens and be cognizant of the small guys out there because it really hurts us. It is what we want to do, but just that administrative overhead is massive. We are not a Zscaler. We are not all these companies. We have a 10 person security team working 15 hours a day trying to do the right thing. I thank you for the time.

Senator PORTMAN. Yes, that is great input. Thank you. It is about size, but it is also about degree of risk.

Mr. FISIC. Right.

Senator PORTMAN. So you could be a small company but be in a highly sensitive area, high risk area in terms of your data. Vice versa, you could be a larger company, a for-profit company that does not have that kind of risk. That is very helpful, and that goes to the compliance burdens.

Again, we want to end up with the best services being provided and do it at the most cost-effective way possible and then taking into account this increasing issue of foreign interference and being sure you are doing everything to avoid the foreign hackers from getting into your system and getting into our cloud.

Thank you, Mr. Chairman.

Chairman PETERS. Thank you, Ranking Member Portman.

Just kind of as a wrap-up question, I am going to ask each of you to respond. We will start with you, Mr. Stern and then Mr. Nodurft. We will start at that end of the table and work the other way around.

As we are writing legislation and thinking of policy, I think it is always really good to think about how you measure success, what is a successful program. If we were to pass this bipartisan legislation that we have before us right now, I would like each of you to tell me what you think the single most important, relevant indicator of success will be if we look back at what we have done. Two or three years from now, looking back, what is going to be the single most important, relevant indicator of success for the FedRAMP program? Mr. Stern, if you would give me your thoughts on that.

Mr. STERN. Sure. For me, the single most important indicator of success, if we look back on it, will be transparency in the supply chain for the Federal buyer, simple as that.

Chairman PETERS. OK. Great. Mr. Nodurft.

Mr. NODURFT. Thank you, Senator. New and emerging technology companies feel as though that there is market certainty around the FedRAMP program enough to invest in the security measures necessary to enter the Federal marketplace. I think that lowering the barrier and increasing the number of authorizations available and making that emerging technology, accessible to the Federal agencies that need it is going to be a big marker of success.

Chairman PETERS. Great. Mr. Kovac.

Mr. KOVAC. Thank you, Mr. Chairman. In my opinion, I think when you look at reciprocity it is going to be—reciprocity and reuse, I mean. Assuming that we resolve the security questions which are extremely important. I hope you know that and feel that I understand that. But this reciprocity, agencies being able to reuse something that is trusted and something that is being monitored on a monthly basis and being able to be quick to market.

But also reciprocity, as I stated earlier and I wanted to bring back up, is when the community itself bonds together to help other CSPs, which you are seeing. Today there is a couple of large players and a couple of moderate players have joined together, and they have built this ATO as a Service. What it is, is it helps small companies that are ISVs, that could not afford it normally, come in and buy infrastructure off one of the hyperclouds, buy their consulting off one of the big time 3PAOs, buy the security, say, off of a Zscaler and buy the SIM and the data login off of a Splunk or a,

SomaLogic. They are buying their ITSM off ServiceNow and being able to get that prepackaged product.

The fact that the industry has come together to do this has shown the belief in the industry, and that is reciprocity working two ways. It is reciprocity working for the agencies and then the CSPs giving reciprocity to each other and joining together. I should say 127 different applications of our cloud being used by third party people that are not the agency that they have used to get their FedRAMP, to get Zero Trust as part of their FedRAMP offering. Those are stunning numbers, and I think that is a very important place.

If we can make that work, if we continue to grow that community, we could lower cost, decrease time to market, and make the reciprocity reuse issue become just key. So that is my No. 1.

Chairman PETERS. Great. Thank you. Mr. Fisic.

Mr. FISIC. I have to echo what Mr. Kovac said. It speeds resolution or certification, automation, true risk focus, and putting the resources toward that and optimizing the process. To me, the most important thing we could do is continue focusing on that, address the risk and automate in every way that we can to speed the compliance process, continuous monitoring, and all those things. I think that is vital to my organization and many others. Let us streamline this and standardize it, and let us ingest it as a matter of course without creating additional risk for organizations.

Chairman PETERS. Great. Thank you. Mr. Mill.

Mr. MILL. There is a lot of factors that go into making FedRAMP successful because it has multiple goals of security, effectiveness, bringing the best tools into government. The way that I would look at it is to take from the vantage point of people inside of an agency who want to use those tools.

In a successful FedRAMP program, people inside of an agency can look around and they can see, there is this awesome tool that has been on the market now for a few years. It is leading. It would dramatically improve how we work. It would change the shape of our operations.

In a successful world, that is a routine thing. That is not a huge ask inside that organization because of all of the factors together, because the chief information officer is used to working with cloud providers. There is high trust in the FedRAMP program and what goes on behind it, and the bureaucratic path inside these agencies is well-trod. If it is already a use in the Federal Government, then all the better, right? That is a natural, easy thing for people to do.

One thing we would look to see whether it is successful, is whether that is something that people continue to exercise as an option.

Chairman PETERS. Thank you. Mr. Shive.

Mr. SHIVE. I am the IT guy, so we measure everything. What I would propose is some sort of value measure across four really easy-to-understand domains.

Velocity. Are we increasing the velocity of authorizations through automation and optimized processes, things like that?

Quality. Is the cybersecurity posture of the Federal Government better afterwards than beforehand? Are we more agile? Are we more responsive in response to the threat that we see?

Costs. Are costs headed in the right direction through reuse and through optimization of the program?

Then the last would be stakeholder experience. Do our industry partners, do our agency partners, do the compliance arms of government, NIST and stuff, do they all say that the program is easier to use, easier to understand? Is it more effective? That takes surveying those groups on a regular basis and measuring that over time. Classic value index-type thinking.

Chairman PETERS. Very good. The last word, Ms. Mahan.

Ms. MAHAN. Thank you. I could not agree more with my fellow panelists here. Continue to be transparent. Trying to usher as many cloud products through this process as efficiently as possible. Incorporating automation. Continuing to increase agency adoption as well as driving that reuse factor. That "do once, use many times" is something that we want to continue to see and continue to push limits across government.

There is an incredible amount of transparency that is provided through this process, really putting security at the forefront of any agency and looking at these security materials, looking at the audits, and making that risk-based decision to use that given product. It is a combination of everything that my fellow panelists have said today moving forward.

Chairman PETERS. Wonderful. I would like to thank each and every one of you again for participating in the roundtable. It is an important subject. It is a complex subject. Appreciate all of your involvement in this and your willingness to share your expertise with the Committee as we work to address this issue.

So with that, our roundtable is now adjourned. Thank you so much.

[Whereupon, at 3:44 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Peters
FedRAMP Roundtable – November 30, 2021

Today, I'm pleased to have representatives from both government and industry here to discuss the Federal Risk and Authorization Management Program (FedRAMP) and our Committee's bipartisan bill – S. 3099, the *Federal Secure Cloud Improvement and Jobs Act of 2021*.

Thank you all for attending. The goal of this meeting is to have a conversation with key stakeholders who can share their unique insights on how FedRAMP helps agencies adopt innovative cloud technologies while ensuring robust security for Federal data and citizen information.

I appreciate Senators Hassan, Hawley, and Daines for co-sponsoring this bill, a version of which has passed the House and is already included in their NDAA package.

Our bill is a comprehensive, consensus set of reforms to drive quicker, more secure of commercial cloud capabilities in government, which will improve agency cybersecurity, empower agencies to deliver modern digital services to citizens, and expand American leadership in cloud technologies.

I look forward to discussing those reforms with the excellent group we have convened here today. With that, I will turn it over to Ranking Member Portman for a brief opening statement, followed by short introductory remarks from each of our participants.

Opening Remarks [as prepared]
Ranking Member Rob Portman
FedRAMP Reform: Recommendations to Reduce Burden, Enhance Security, and Address Inefficiencies in the Government Cloud Authorization Process
November 30, 2021 @ 2:30pm

I am glad we're holding this roundtable today to examine FedRAMP. Thank you to our participants for joining us today, and especially to Mr. Fisic who joins us from OCLC in Dublin, Ohio. We appreciate your attendance here today to provide your insights on your experiences with the FedRAMP program.

FedRAMP's "do once, use many times" framework has many benefits. For example, the reuse of authorized cloud systems has helped the government avoid an estimated $716 million in costs.

The current program, however, also has weaknesses which have left it vulnerable to foreign-backed hackers targeting cloud systems, like China and Russia. Right now, we do not have sufficient safeguards in place to identify and prevent foreign interference in our cloud systems and that must change before we codify this program.

This is especially important in light of FedRAMP's emphasis on reuse and the program's influence beyond the federal government. State and local governments often procure FedRAMP authorized products because the FedRAMP label implies these products and services are secure.

Further, FedRAMP heavily relies on the security assessments performed by private sector third-party assessment organizations. Surprisingly, cloud service providers choose

which 3PAO will conduct the security assessment of their cloud system -- and pays the 3PAO for the assessment.

Finally, despite best efforts to improve the program, FedRAMP still suffers from high costs, long timelines, and inconsistent review processes across agencies. As a result, federal agencies have fewer cloud service offerings to choose from compared to their private sector counterparts, hindering agencies from procuring the best service for their needs. As of today, there are roughly 240 FedRAMP authorized providers, compared to the thousands available in the private market.

I look forward to a productive conversation on how to address the inefficiencies and burdens in the FedRAMP program, and how to improve the security posture of the government's cloud systems.

Thank you.

(Oral & Written Statement)

FedRAMP Roundtable Discussion

Statement of Ashley Mahan
Acting Assistant Commissioner, Technology Transformation Services

U.S. General Services Administration

Before Members of the Senate Committee on Homeland Security and Governmental Affairs

November 30, 2021

Good afternoon, Chairman Peters, Ranking Member Portman, and distinguished members of the committee. I thank you for the opportunity to participate in this roundtable today alongside my colleague, David Shive, the Chief Information Officer (CIO) of GSA and a member of the Joint Authorization Board (JAB).

I am Ashley Mahan, the Acting Assistant Commissioner of the Technology Transformation Services (also known as TTS) Office of Solutions within the General Services Administration (GSA).

I have spent most of my career dedicated to cybersecurity and mitigating risks to the security of federal data. I have worn several hats—from writing System Security Plans (SSPs), preparing for security audits, and serving as an Agency Information System Security Manager (ISSM) to leading FedRAMP. I've also had a chance to work with the many different types of professionals involved in the end-to-end process—from cloud architects, incident responders, auditors, and engineers to acquisition specialists and c-suite executives. They are always at the top of mind as we define improvements and develop the strategy for FedRAMP.

The program's success is largely based on our partnerships. We've listened to our partners and they've been instrumental in how we have evolved and run the program today. We're about to celebrate the 10 year anniversary of FedRAMP. Along the way, we've made steady growth and the pace at which companies get products authorized by FedRAMP has improved. In the last three years we have more than doubled the number of authorizations, from 100 to 240, as well as more than tripled the number of re-uses of FedRAMP-authorized cloud products (from 918 to 2864). The program's growth has even greater urgency given the continued demand for secure cloud technology and the need to work remotely.

As I look ahead to the future of FedRAMP, automation and modernizing processes will be the focus of the program's strategy. Meaningful and lasting change will happen only with continued collaboration with our government and industry partners. We'll continue to leverage the insights of the cybersecurity community in order to solicit feedback as we continue to implement automation and modernize FedRAMP processes. Our work is never done in this dynamic space. FedRAMP is committed to continuous improvement and transparency, driving the need to cultivate strong working relationships across industry and the federal government community in support of securing cloud technology.

(Written Statement)

FedRAMP Roundtable Discussion

Statement of David Shive
Chief Information Officer, General Services Administration

U.S. General Services Administration

Before Members of the Senate Committee on Homeland Security and Governmental Affairs

November 30, 2021

Chairman Peters, Ranking Member Portman, and members of the committee, my name is David Shive, and I am the Chief Information Officer at the U.S. General Services Administration (GSA), as well as one of three Joint Authorization Board (JAB) Members for FedRAMP. I am pleased to be here today to discuss the important role and impact that FedRAMP plays for the federal government.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) was established in 2011 to provide a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government. Instead of each agency having to review and approve their individual cloud computing solutions, FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. It reduces redundancies across the federal government by creating a "authorize once, leverage many times" model for cloud products and services.

FedRAMP ensures that essential security controls are properly implemented on cloud systems that process, store, and/or transmit government data. These security controls cover

management, operational, and technical risks, including safeguards to combat cyber threat and supply chain risks.

Risks can be effectively managed through the application of appropriate security countermeasures provided by FedRAMP. They can also be addressed by ensuring that when incidents occur, they are managed, mitigated, and responded to in a manner consistent with FedRAMP and Federal incident response requirements, ensuring that the risk is not spread throughout the government.

Role as Joint Authorization Board (JAB) Member

As a member of the JAB, I work closely with the Chief Information Officers from the Department of Defense (DOD) and Department of Homeland Security (DHS) to oversee FedRAMP. Together, we manage a government-wide approach to address the security needs associated with placing federal data in cloud computing solutions.

The JAB serves as the primary governance board and provides provisional joint authorizations of FedRAMP packages submitted by Cloud Service Providers (CSPs), assessed by FedRAMP Third Party Assessment Organizations (3PAOs), and reviewed and validated by JAB Technical Representatives from DOD, DHS, and GSA. The approved cloud solutions can then be leveraged by individual agencies across the federal government to grant an Authority to Operate at their respective organizations.

FedRAMP Enables Technology Modernization

GSA's mission is to deliver the best value in real estate, acquisition, and technology services to the government and the American people. Our priorities are to deliver better value and savings, serve our partners, expand opportunities for small business, make government more sustainable, and be a leader in innovation.

To support these initiatives, my organization is delivering modern cloud technology that provides a secure environment for doing business, while ensuring that both IT and business continue to run efficiently. GSA leverages numerous cloud providers through FedRAMP that are a mixture of Software, Platform and Infrastructure as a Service—depending on the business needs of our customers.

Federal agencies are increasingly looking to the cloud to transform the way employees and the public interact with the government to receive services. FedRAMP empowers agencies to use modern cloud technologies to drive transformation efforts, with an emphasis on security and protection of federal information.

FedRAMP Outcomes

Under FedRAMP, we have seen an exponential growth in the use of cloud solutions across the federal government, creating significant cost savings and improving service delivery to the public. The program has provided a standard for assessing and continuously monitoring the security posture of these cloud services. By creating the "authorize once, leverage many times" model, federal agencies have been able to safely reuse cloud technologies that have received an authorization to operate.

Conclusion

Thank you for the opportunity to appear before you today to discuss FedRAMP and its important role in the federal government. GSA is happy to work with the Committee on legislation to provide new opportunities to mature and advance the future of FedRAMP. I look forward to answering any questions you have.

Securing your digital transformation

Written Statement of

Stephen Kovac
Chief Compliance Officer & Head of Global Government Affairs
Zscaler, Inc.

US Senate Committee on Homeland Security and Governmental Affairs
Roundtable: FedRAMP Reform: Recommendations to Reduce Burden, Enhance Security, and Address Inefficiencies in the Government Cloud Authorization Process

November 30, 2021

Thank you, Chairman Peters and Ranking Member Portman for holding this roundtable on FedRAMP reform.

My name is Stephen Kovac, and I lead global compliance efforts for Zscaler. Having worked with the FedRAMP Program Management Office (PMO) in a variety of capacities since the program was established 10 years ago, I have first-hand experience of the importance of FedRAMP to helping the federal government secure its systems and networks, as well as some of the challenges the program has faced as it has grown and evolved.

Zscaler's mission is to make the cloud a safe place to do business and empower organizations to realize the full potential of the cloud and mobility by securely connecting users to applications anywhere, from any device. Zscaler provides secure cloud computing services to Fortune 500 companies as well as federal agencies. Two of our products used across the federal government -- Zscaler Internet Access and Zscaler Private Access -- are certified (or "ready") at the FedRAMP "High" level.

FedRAMP serves as a critical gateway to secure cloud computing in the federal government, providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud solutions. This benefits federal agencies that leverage FedRAMP-certified solutions and cloud service providers (CSPs) like Zscaler that provide these secure solutions to government agencies. The public today increasingly relies on the Internet to access government information and services, and they demand that these services be secure. Over the last 18 months, as the COVID pandemic changed all of our working habits, cloud-based tools allowed many agencies to seamlessly shift from in-person to remote work and do so in a safe and secure manner. Yet the increase in remote work has also expanded the attack surface, with federal systems and networks facing increasingly sophisticated and relentless cyber threats on a daily basis. There is no issue more critical than for federal agencies to be able to trust that the cloud solutions they procure are secure and held to the highest standards. FedRAMP helps provide that assurance.

Zscaler supports the *Federal Secure Cloud Improvement and Jobs Act* (S. 3099) and appreciates the efforts of this committee and others in Congress to move the legislation forward. The bill is critical for the program itself, in that it will drive continuous improvement of the program, while helping ensure that federal agencies have access to the cybersecurity tools needed to protect them from today's ever-evolving cyber threats.

Furthermore, enacting S.3099 will help the FedRAMP PMO better serve the companies and agencies that rely on it to ensure they are delivering the highest level of security. As the committee is aware, the bill includes provisions aimed at increasing reuse of FedRAMP authorizations across government as well as reducing the time to deployment and associated costs. For companies such as Zscaler, increasing reuse and reciprocal treatment of existing FedRAMP certifications is a key component of S.3099. If enacted, the legislation's "presumption of adequacy" provision will help FedRAMP more closely live up to its original vision of "certify once, use many times."

When it comes to the criticisms we sometimes hear about the program -- for example, that it takes too long or costs too much to achieve certifications -- it is important that the committee recognize that some of the complaints directed at FedRAMP are not always about problems created by FedRAMP or something that FedRAMP can solve. As you consider reforms to FedRAMP, I encourage you to separate policy areas where FedRAMP can continue to make improvements, such as accelerating the authority to operate (ATO) certification process, from complaints about the federal acquisition process itself or the underlying security requirements for FedRAMP which the PMO does not have control over.

Thank you for inviting me to participate in today's roundtable. I look forward to your questions.

Biography of Stephen Kovac

As Chief Compliance Officer & Head of Global Government Affairs at Zscaler, Stephen Kovac has responsibility for overall strategy, productizing, and certification of the Zscaler platform across all global governments. He also runs the global compliance efforts and government affairs for Zscaler.

Stephen is a 27-year veteran of the information technology and security industry with extensive experience in public sector, compliance, and government affairs. Prior to Zscaler, Stephen served as EVP of Strategy and Public Sector for VAZATA, a FedRAMP certified cloud provider, as VP/CSO for BT Security, Vice President at Terremark Federal, a Verizon Company, and as Vice President of Verizon, Public Sector. He is a frequent speaker, blogger, and highly quoted author on federal security and certifications. Stephen has been most recently recognized for efforts and collaboration within industry and government as a 2019 MeriTalk Cyber Defender, 2020 FedScoop 50 Finalist, and a 2020 Fed100 Winner.

Written Statement of

Ross Nodurft

Executive Director

Alliance for Digital Innovation (ADI)

US Senate Committee on Homeland Security and Governmental Affairs

Roundtable: FedRAMP Reform: Recommendations to Reduce Burden, Enhance Security, and Address Inefficiencies in the Government Cloud Authorization Process

November 30, 2021

Thank you, Chairman Peters, Ranking Member Portman and members of the Committee for holding this roundtable on FedRAMP reform.

My name is Ross Nodurft. I am the Executive Director of the Alliance for Digital Innovation (ADI), a coalition of innovative, commercial companies whose mission is to bring IT modernization and emerging technologies to government. ADI engages with policy makers and thought leaders to break down bureaucratic, institutional, and cultural barriers to change and enable government access to secure, modern technology that can empower a truly digital government.

ADI focuses on four key areas in our federal advocacy efforts – accelerating technology modernization in government, enabling acquisition policies that facilitate greater use of innovative technologies, promoting cybersecurity initiatives to better protect the public and private sectors, and improving the federal government's technology workforce. Each of these areas must work closely with each other to allow for government mission owners and technology providers to partner with industry to build a modern, digital government.

ADI's members include some of the leading technology and professional services providers to the public sector, many of which have gone through the FedRAMP accreditation process or are working to achieve FedRAMP accreditation. These technologies underpin the federal government's modernization efforts and provide the backbone for many agencies' zero trust architectures and plans.

Given our areas of focus, ADI applauds the work that Congress – and the members of this committee – have done to evaluate and craft legislation that can accelerate some of the changes needed to enable secure access to modern and emerging technologies. S. 3099, the *Federal Security Cloud Improvement and Jobs Act of 2021*, and its House companion, H.R. 21, if enacted, would provide stability around the FedRAMP accreditation process and authorize the resources needed to drive many of the reforms called for by the Government Accountability Office (GAO)[1] and Inspector General of the General Services Administration (GSA). [2]. Over the last two years, ADI has expressed its support for codification of FedRAMP. More specifically, ADI has stated and maintains its support for:

- the authorization of additional sustained resources to increase the number of FedRAMP authorizations;
- additional collaboration with industry;
- driving reuse and reciprocity of FedRAMP accreditations across the federal government;
- adoption of automation throughout the FedRAMP process; and
- the market certainty that codification provides for innovative companies seeking to access the federal marketplace.

[1] https://www.gao.gov/assets/gao-20-126.pdf
[2] https://www.oversight.gov/sites/default/files/oig-reports/A170023_1.pdf

There are a few provisions of the *Federal Security Cloud Improvement and Jobs Act of 2021* that I would like to highlight; these provisions will help the FedRAMP program achieve its goals and accelerate its planned improvements.

First, the authorization of $20 million annually for five years represents a good start to fully funding the program. This initial increase will provide much-needed, consistent resourcing to hire additional individuals with the technical skills necessary to review and process authorization applications. These resources, coupled with increased use of automation, can quickly expand the number of provisional authorizations issued by the proposed FedRAMP governance board.

Second, the establishment of the Federal Secure Cloud Advisory Committee has the potential to create a consistent, formalized feedback loop through which industry can partner with GSA and the federal agencies to drive consistent improvements and quickly elevate and adjudicate concerns as they arise. We strongly urge OMB, GSA, and CISA to leverage this body proactively and regularly to accelerate cloud adoption across the federal government.

Finally, codification of the FedRAMP program further underscores the importance of the program while creating market certainty that investment in FedRAMP accreditation will mean something in the public sector marketplace in the future. In addition to adding stability to the program through codification, S. 3099 also reenforces public sector market certainty by driving accreditation package reuse by other agencies.

Resourcing the FedRAMP Program

For much of the past decade, funding for the FedRAMP program has remained flat while the program processed and accredited over 240 cloud services. This program has become an essential part of the federal government's cloud adoption journey and remains integrally important to maintaining high cybersecurity standards. The Biden Administration's Executive Order 14028 on Improving the Nation's Cybersecurity[3] specifically calls out the cloud as an important way to raise the bar on security across public sector entities and identifies several actions that the FedRAMP program needs to take to facilitate secure adoption of cloud services.

However, the program's ability to make those changes and to continue to drive secure cloud adoption is contingent on proper resourcing. A FedRAMP accreditation through either the Joint Authorization Board (JAB) or Agency process requires annual paperwork and re-authorizations as part of the continuous monitoring process. In fact, every time a cloud service provider makes a significant change or update to its cloud service offering,[4] it must submit a change notification form to the FedRAMP program management office (PMO) prior to implementing that change. These real time updates and product improvements are at the core of what makes cloud service offerings more scalable and secure. Yet, each of these changes must be manually adjudicated by FedRAMP. Today, this means that GSA must make a choice between accrediting new cloud services at a faster rate and dealing with the backlog of re-authorizations and change

[3] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[4] https://www.fedramp.gov/assets/resources/templates/FedRAMP-Significant-Change-Form-Template.pdf

requests from services that were approved during the past ten years. These resourcing choices and trade-offs can be reduced through additional funding.

S. 3099 begins to address these resourcing constraints through an authorization of $20 million per year for five years, which is a good down payment on the process. However, ADI believes that even more funding is necessary to turn FedRAMP into the cloud security accreditation program the federal government needs to facilitate the significant shift to cloud services that the Biden Administration is championing.

Federal Secure Cloud Advisory Committee

A formal industry voice has been missing from the FedRAMP conversation since the very beginning. A public/private sector advisory committee may not have seemed necessary when the program began ten years ago. However, the cache that the FedRAMP brand commands in the federal marketplace coupled with the billions of dollars in annual Federal IT spend make it essential for government and industry to work together to improve the program.

Cloud Service Providers (CSPs) have been reluctant to provide feedback to GSA for fear of jeopardizing their relationships with program management staff and accreditation officials. While the FedRAMP program and GSA have reached out and worked with CSPs on an ad hoc basis, there has not been an official forum to formally identify and collaboratively discuss and address the impact of policy changes. Further, agencies outside of those represented by the JAB have not had an opportunity to shape the FedRAMP process despite being key stakeholders

and customers of the provisional authorizations to operate (P-ATOs) granted through the program.

The ability to consistently engage with FedRAMP's key stakeholders can be addressed, in part with additional resources. That said, the direction and formal authorization of the Federal Security Cloud Advisory Committee in S. 3099 will provide essential structure that can facilitate a better understanding of the impact of changes in policy as well as a dedicated forum to discuss programmatic improvements that will maintain or improve security while increasing agency access to secure cloud services and products.

Encouraging Reuse and Reciprocity

The Federal Information Security and Modernization Act (FISMA) of 2014[5] requires every federal department and agency to own its own risk. This incentivizes risk aversion across government authorizing officials and IT leadership. While S. 3099 recognizes the requirements of FISMA, it moves agencies in the right direction by codifying the "presumption of adequacy" of the security assessment that underpins a FedRAMP accreditation. Further, S. 3099 requires agencies to reuse the security assessment package whenever possible. This is an important mandate that will help continue driving private sector investment in the FedRAMP accreditation, since reuse is key to the program's value.

[5] Public Law No: 113-283

ADI members believe that having a security accreditation program that will remain in place across administrations helps companies who are considering the investment in FedRAMP. Reinforcing that investment by driving reuse of a product or service's underlying security package also provides more market incentive to pursue a FedRAMP accreditation.

However, government can go even further by providing meaningful reciprocity across compliance regimes. FedRAMP accreditation is already the foundation for cloud security across the public sector. By underscoring FedRAMP as the gold standard in cloud security and encouraging reciprocity in the public sector marketplace, additional modern and innovative companies can make the business case for investing in the FedRAMP process. The more companies are accredited, the more easily government can move away from legacy technology and embrace secure cloud-based emerging technology.

Authorizing Automation

For the last ten years, the FedRAMP process has relied on manual, paper-based compliance processes to build, assess, update, and review authorization packages. This cumbersome practice has continued to underpin – and often slow down – the accreditation process, even as the use of automation, machine learning, and artificial intelligence has proliferated in other parts of the government. The same manual process also drives the review of any significant change request. These manual reviews quickly consume the resources available to FedRAMP causing additional delays for existing services and preventing new CSPs from moving up in the accreditation queue.

While the GSA and NIST have been working closely on a series of automation procedures, the accreditation process still relies on time-consuming, manual processes. S. 3099 requires GSA to review the automation procedures that are currently being developed and tested and, within a year of enactment, establish a means for automating assessments and reviews. This will mark a pivotal change for the program and free up FedRAMP resources who are overburdened by the current manual processes.

Conclusion

In conclusion, ADI supports the efforts of the committee to invest in and improve the FedRAMP program. We are encouraged by the committee's work on S. 3099 and applaud the bill's efforts to increase funding for the FedRAMP program, create a formal process for industry engagement, increase use of automation across the program, and provide market certainty through codification.

ADI appreciates this opportunity to participate in today's roundtable and share our insights on improving cloud adoption in government. I look forward to any questions you might have.

Jeffrey Stern, Chain Security - Opening Statement

Good afternoon. I want to thank the members of the Committee for inviting me to participate in the Committee's FedRAMP Roundtable.

I am Jeffrey Stern, and I am the CEO of Chain Security. Chain Security is a Reston, Virginia based consulting engineering firm that is engaged in two related areas:

1. Securing the supply chains of U.S. commercial high technology companies from interference by foreign parties
2. Compliance of companies that are regulated by the Defense Counter - Intelligence Security Agency (DCSA) or the Committee on Foreign Investment in the United States (CFIUS).

Chain Security's consulting practice is informed by the unique combination of skills and backgrounds of our team. Our technology team includes members who have deep commercial product development and delivery experience in Silicon Valley. The company includes team members who have recent and deep experience in U.S. Government security practices and policies.

We bring extensive government security experience from organizations such as DOD's CFIUS Office, DHS, the Federal Communications Commission (FCC) and the FBI. This includes team members with recent experience at DHS's Cybersecurity and Infrastructure Security Agency (CISA).

Most of our CFIUS and DCSA related work is focused on the development and implementation of national security mitigations that the U.S. Government has required of our clients.

I am personally engaged in the area of CFIUS investigation of foreign technology companies on behalf of DOD's CFIUS Office.

The supply chain security information related to FedRAMP that Chain Security has presented to the staff of the Committee is based upon observations we made over several of our consulting projects in 2019 and 2020. It is possible that GSA's FedRAMP program have already addressed some of our observations.