*7435301*

# Federal Secure Cloud Advisory Committee September 2024 Meeting

*September 12, 2024*

*CONFIDENTIAL ROUGHLY EDITED REALTIME FILE*

*Compliments of Birnbaum Interpreting Services*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

*This file was created in real time by a Realtime Captioner. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. A consumer should check with the presenter for any clarification of the presentation.*

*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**

>> Good afternoon, welcome to the September 12, 2024 meeting of the Federal Secure Cloud Advisory Committee or FSCAC. My name is Michelle White. And I am the designated DFO for this Advisory Committee. I want to thank all of our presenters, and stakeholder joining us including those who provided public comment. Public comment submitted via the FSCAC public comment form by Wednesday Wednesday, September 4 have been provided to committee members.

Before we start there are few things that you should know. This meeting is being recorded via Zoom. This is an Advisory Committee, the statutorily required under the James-- national defense Authorization Act for FY 2023. And formally established under the Advisory Committee or FSCAC as the official filing date of February 28, 2023.

This committee is considered a Federal Advisory Committee and governed by the requirements under FSCAC. My role as the trough is manage the day-to-day administration of the committee, attend committee meetings and ensure that the committee operates in compliance with FSCAC. Duties of this committee include provide recommendations to the administrator, board, and agencies on the technical operational matters regarding the secure adoption of Cloud computing products and services.

The majority of the work of this committee will be focused around the federal Authorization Act of 2022 statutory requirements.

And the purpose is specifically to one, examine the operations of-- and determine ways that authorization processes can continuously be improved. Two, collect information and feedback on agency compliance with implementation of FedRAMP requirements and three, service the form that facilitates communication and collaboration among FedRAMP state community.

I will go through a roll call. Let me know if you are present by stating here.

>> [Roll Call]

>> Larry Hale.

>> Here.

>> Thanks, Larry. Michael-- Carlton Harris.

>> Here.

>> Kayla--

>> Here.

>> Josh Krueger. Daniel Pane.

>> Here.

>> Marcy.

>> Here.

>> [Roll Call]

>> It does look like we have a quorum established. So I'll go ahead and review our purposes, outcomes and agenda topics for today. Just for everyone's awareness of the purpose of today's meeting is twofold. We will get an update from OMB and receive stakeholder input on our top two priorities for the year.

The outcomes for today are a shared understanding of OMB's impact of OMB's FedRAMP memo and shared understanding facing industry and agencies during the FedRAMP authorization process.

Our agenda today is as follows, welcome call to order-- and then we'll jump straight into our public comment period until 12:25, and then take some quick Chair remarks until 12:30 and hear from OMB and Q&A session until 1:15. And take a 15 minute break until 1:30.

And we'll just go ahead and move, right into our panel discussions for today. Each time approximately an hour starting with the industry panel discussion will include call service providers and industry representatives and ending with a panel discussion with the liaisons. Key takeaways and closing remarks no later than 4:00PM.

A few housekeeping items for committee members. Be sure to identify yourself before speaking so listening online, those or reading the minutes after the meeting will know who made which comment. And this is a virtual meeting. Please make sure that your microphone is on mute any time you're not speaking. When it is time for the committee to ask questions and you'd like to raise your hand, please click on reactions button in the menu bar and then click raise your hand.

And if you remember to click, lower your hand when done speaking. I would appreciate it. Lastly if you are not a committee member, please hold all of our comments until the public comment period and ensure that your microphone is on mute otherwise.

Great. We will go ahead and move into you are public comment period. at this time I would like to welcome the members of the public to share their comments. To our speakers, note that a timer will be indicated on the screen, with your timer remaining. Each speaker will be allotted 3 minutes to make their comes. We will be interrupting speakers who exceed three main minutes to speak. Be respectful of the time. As a reminder, all of the public comments submitted by Wednesday, September 4 were presented to the committee members prior to this meeting. With that I'd like to get started. And I'll begin to call on people who have submitted comments online, and in indication they are in attendance today, and if we have a remaining time, we will move to other people.

Do we have Ryan Gutwin in the meeting who would like to speak? All right. Great. Chris Dietrich? We have somebody who listed themselves within the initialed K. M. All right. We do have somebody who provided comments with the name of Anne Murray\_ --\_. All right. Jennifer Pierce.

We also have somebody named-- who submitted comments. Ken White? And finally Scott\_ --\_. Okay.

If anyone else would like to make a comment, a public comment today, please go ahead and raise your hand. And I can call on you in the order that you raised your hand. I will not seeing anyone--

>> I'd like to make a comment but I can't seem to raise my hand on the screen here.

>> I have my hand up as well.

>> We have who is speaking just now, go ahead.

>> You go. I'll go after you. I don't mind. You go first.

>> Okay. Yes. So I'm Cal, the CTO. I want to say I appreciate making comments here. In the FedRAMP program, the Federal Government and CSP, providers, we all invested heavily in the knowledge which the agencies that use it are able to compute it. We are proud and excited of the program. We got authorized in early 2022. Started in 2018. We're concerned, however that we are seeing many agencies that require FedRAMP solutions for project management systems or they're not mandating the contractors that they need to be utilizing systems that are authorized.

And we see the rules does create security vulnerabilities and results in inefficiencies which are because we can provide the best possible pricing due to what we have to absorb.

A little further than that, an the vulnerability risk, it's significant. We see, you know, FedRAMP promote secure solutions without a framework in place, there are ad hoc controls. And we see that in industry when there are solutions that have open issues and no way to resolve without anything in place to enforce it such as FedRAMP. Inefficiencies, there's business cost FedRAMP and we have to do data calls. We have to respond to those in systems and things that come up that something in our team has to track down. We know based on FedRAMP we have things like inventory in place and protocols but we still have to go through the exercise of working on-- we also note that some of these can be intense and a lot of work involved. So you know, sum this up, we believe that the mission of FedRAMP is critical and there is tighter enforcement of the adoption of FedRAMP solutions that should be a priority. Thank you.

>> Colin, this is Matt. What was your company? What are you CTO of?

>> CTO-- (?)

>> Got it. Thank you, Colin. Terry, if you would like to go ahead.

>> Thank you. Can you hear me?

>> Yes, we can hear you.

>> Okay. Good afternoon, FedRAMP Cloud Advisory Committee members and those who have joined virtually. Thank you for having me.

I'm Terry-- CEO of the trading companies, the tiny W-- in the U.S., Canada and Brussels many of you remember me from previous comments. I spoke at the very first of these events in 2023.

I've been with the IT solution business for more than 20 years and personally for me 50 years. Had a connection to FedRAMP that may be the deepest of any organization as we made our commitment to FedRAMP standards in 2017 and never wafers from that goal. I like to say that what we've done is completed when I call the full FedRAMP 3PA. Readiness, the Czar, and agency APO from the United States Senate.

But then we come to the real crux of the matter for Cloud service providers. FedRAMP security standard for Cloud compute has been around since 2011. Our work since 2017 through FedRAMP approval for several million dollars. Since 2011 only about 400 organizations have gained FedRAMP approval. And of the area in which we work, platform is a service, 2011 until now only 48 have been approved.

Obviously, up until now, FedRAMP certification has been a bureaucratic nightmare delay. FedRAMP is a law. It's been depending on a delivery model where Cloud service providers require a very particular invitation process to take part. The nice way to say it is it's a regressive policy that has limited FedRAMP's success and means FedRAMP certifications are dominated by large prime contractors.

In our next code, a small business is really a very large business. To really, with ten people worldwide is the smallest organization to ever qualify for FedRAMP. What bothers me about this process is it reminds me of the days when one was invited to a dance and they couldn't dance until they had somebody ask them to dance. Fortunately, not all FedRAMP news is bad. FedRAMP working with NIST frameworks and the Department of Defense has expanded roots to certification and established equivalency of standards and various constituent groups. To recommend therefore use our ATO for certifications by this alternate path and by inherited controls for what I call the self-nominated.

They will no longer be required to get an invitation to apply and can via framework and digital clones and inherited controls--

>> Terry.

>> This service move forward.

>> You're out of time, unfortunately.

>> I will provide the remainder of my talk by comment. But I would like to say, that our goal is to certificate more than a thousand organizations in the next month.

>> I'm sorry. You're out of time. We need to move on.

>> No, you don't. There's no one waiting.

>> There is an entire agenda waiting. And we are open for public comment in writing. And we've had a lot of great public comment in writing. We appreciate. We read them all. I appreciate the hearing from the public, absolutely.

>> Yeah. And you haven't--

>> Thank you. Susan, please go ahead and speak.

>> Yes, I'm Susan. One of the Cloud Service providers we are working with has started telling us that they're experiencing challenges in being able to procure a third party assessment organization. They've said that many of the 3 PAOs have so much work that they have, that they're not able to bid on new work. I was not sure, I have not heard this before. I want to put that out there to see if other cloud providers are having issues with that or other agencies are hearing that. Thank you.

>> All right. Thank you so much. Are there any other public comments? Thank you so much for your public comments. This really concludes this portion of the agenda.

We will now go ahead and jump into our topic of chair liners. Larry, welcomes this committee Chair, I would like to invite you to make any remarks you'd like at this time. I'll be happy to answer questions that come up. Larry, please go ahead.

>> Larry Hale: Thanks, Michelle. And again, thanks for the public comments. We do have a full agenda today. And we have received a lot more public comments in writing through the portal, thanks to committee members and others amplifying the message. But we do want to hear from you. And certainly, if it's a detailed comment, we welcome the written comments and appreciate that very much.

To quickly recap our July meeting, we further refined our top priorities and decided to begin developing recommendations for these first two listed on this slide. I'll give everyone a in into re-read this.

We were given tie additional priorities from the GSA Administrator. Specifically to one, identified best practices and recommendations how FedRAMP can make progress with commercial reciprocity. And two, identify what is needed to support adoption to S credit. AL within the agency, GRC ecosystem that need to be addressed. Due to the nature of the content needed and the timeline on these timeline of these on FedRAMP's roadmap, we have to pause working on this right now and address them after working on these two initial priorities first.

As discussed in our last meeting, when the discovery phase of developing our recommendations. In terms of today's agenda our focus is twofold, one on understanding the impact of OMB FedRAMP memo released on August 1. And two hearing from FedRAMP stakeholders both industry and agencies on their experiences and challenges with the current FedRAMP authorization process. These two points will help us in our next meeting further discuss and develop a structure for our report to the administrator and recommendations on these two initial priorities.

While we receive to go from OMB and FedRAMP stakeholders today, please be sure to take notes on specific key information you'd like to company tour, this is to the committee members, you'd like to capture and/or highlight in our report to the administrator. At the end of this et mooing, we'll capture those takeaways that we potentially like to add to the initial draft report in preparation for the next et mooing.

Does anyone have any questions before we proceed?

All right. Great. One more quick update for everyone. FSCAC looked into getting the social media handles for this committee specifically X and LinkedIn platforms. Unfortunately, GSA is not adding more accounts to X due to the issues with the platform. However we will be getting a LinkedIn account to help further amplify our request for public comment and announce meetings. In addition to the federal register as required by FACA which is great news.

I want to make sure everyone saw the announcement that FedRAMP has a new Director Pete Waterman. If you like to say a few words to the committee, I'm happy to share the floor with you.

>> Fantastic. Thanks, Larry. I would love to. I'm Pete, think 13th day as the FedRAMP Director but my 50 year dealing with the reality of compliance and security and all of the complex government laws, policies and regulations that make these a little bit difficult for those of us in government to do our actions that those in private sector take for granted.

My first couple of months in government, I stated that I could move an entire department into the Cloud in a week by setting up staging environments and starting that process. And then I was like, what's this thing called an ATO? Next thing I knew I had this giant whiteboard full of 50 people I have to talk to to get a get approval. I know how real it is and complicated it is.

On the flip side, I know what you all are arguing. I recently was riding a motorcycle across the country to come back to DC. I found out I had this job. And recordings of these meetings on YouTube basically got me across, Idaho, Montana, North Dakota, and Minnesota over the course of multiple days. Thank you for that.

The thing I'd like to lean into for you all is a reminder that you have an unprecedented opportunity to propose and take measures to improve our community. I believe you can have the biggest impact by focusing specifically on actions that are directed at the entire community to bring the community together rather than on a single portion of the community. There are two things that are really on my mind related to this where I think you are best positioned to help.

The first is communication and collaboration on a technical level. This is the first technical community I've been a part of where I don't have a place where I can see years and years of technical discussion about a control or implementation or housing code works just out there on a forum or website to reference. Instead it all hidden behind 500 page PDFs and LinkedIn post. It's not accessible and not in the open. How will we get the technical people in our community the engineers that are doing the work that it's unreasonable to say, pull up this 500 page document, memorize it and do all the things. That's not how we work at the technical level.

How can we build a community where people go and talk amongst themselves? That's when it's difficult for me to do as a Federal Government. If you give me direction where to participate, I will work with, my office is strategic information on stakeholders make that happen we can interacted directly with you instead of occasionally with a bunch of suits in the room.

Second thing on my mind, and this again, you are all uniquely positioned for this. This is one of the hardest things for me going from private sector to government was understanding how different things are. The most expensive steak I had every eaten was paid for a vendor that my company-- it's personal, right and it's personal relationships. You hire someone because of their personal relationships and what they can get you.

You leverage personal relations in industry so much. Can't do what in government. I can't interact with someone as Pete Waterman. I have to be the FedRAMP Director. This is very complicated. Something a lot of industry doesn't understand and struggles with. And it's something that a lot of government folks don't understand. They can easily get in traps. So one of the things I would also really appreciate from you all, on that just help the community understand so we're not-- private sector is not expecting the same thing from other industry folks from us. And we're not expecting the same thing from other government folks. We need to understand how this all works.

Please help me with that. I don't know if I ran out my time there, Larry. Those are the things on my mind where you can do something I can't do, running my organization inside the government as a representative of government.

>> Pete, I don't think this community or this committee can hear enough from you. So really appreciate it. Welcome to your new role. We're thrilled to have you. And Michelle, for Chair remarks, that's it for me for today. Please take us onto the next; and Michelle, if you're speaking, you may be on mute.

>> Hey, this is Ashley. I can't hear Michelle either. But I am happy to present some slides with my colleague, Laura who is on the line from OMB as well, just need access to be able to present my screen. So whoever may be the person that's showing that or the meeting owner, feel free to transfer screen share access to me or whoever is sharing their screen, if you wouldn't mind stop sharing your screen and I may be able to get in there and do it. Awesome. fantastic. I saw that mouse doing. Appreciate that, Larry.

>> That was D'Arcy.

>> D'Arcy, thanks so much. Let me go ahead and get this teed up. I think there was a hand raised. Was that something?

>> Sorry, Ashley, I'm hitting buttons.

>> Ashley: I want to make sure, everyone can see my screen. Give me a thumbs up.

>> We see your screen.

>> Ashley: Thanks, everybody. I'm going to turn this over to Laura.

>> Laura: Thanks, Ashley, good afternoon every, I am Laura -- Director modernization and data here it the federal chief officer. We released M2410 which modernizes FedRAMP and really excited to be here. And really the intent overall of the memo is to help agencies accelerate online and unlock resources to deliver mission in a modern way.

And next slide, please. And also do you mind moving into present mode, Ashley?

So with the updated memo err trying to drive to an overall feature of FedRAMP where we have improved customer experience, stronger security and risk management, and reduced time and cost to accomplishing the FedRAMP authorization.

So when we talk about improved customer experience, he with want to mick sure we are talking about a more straightforward authorization path for Cloud Service providers and agencies, helping facilitate better transparency and what the process will be, as well as a better transparency and accessibility of FedRAMP authorization packages to agencies when they want to leverage this FedRAMP authorizations.

We're also working with the FedRAMP team to ensure that there's more engagement with a larger technical Pam staff to help support all the efforts and modernization within the memo. And we also really want to make sure that the program is responsive to customer challenges. And in fact the intent of the memo, taking advantage of the fact that the memo is now operating in an environment where there's considerably more SaaS offerings where there previously had been primarily IS offerings.

Next we really focusing on driving stronger security and risk management. You know, while the memo in the statute talks about the presumption of adequacy, we want to make sure all of FedRAMP customers and are engaged in inclusion the cybersecurity across the enterprise and making sure that the security authorization or FedRAMP authorizations meet those security expectations as well as can adapt to novel architectures and complex configurations and also that there may be emerging and novel threats within the course of a FedRAMP authorization. Being responsive to that and driving that security first mentality within FedRAMP.

Then in particular, really making sure that those outcomes are rooted in real-world security needs prioritizing authorization requirements that really drive towards security requirements and where we can find efficiencies and reducing the ones compliance oriented than security oriented.

And as we're operating within this more security first model, Hoving toward a data drive risk management approach especially with our automation efforts that we'll talk about shortly, moving toward how can we talk about aggregated risk, where we can measure risk and look at quantifiable risk reductions and risk mitigations to sort of support that enterprise approach within FedRAMP.

We also really want to make sure that this new FedRAMP process and ecosystem reduces the time and cost in order to meet these security objectives. So you have heard a lot around automated.FedRAMP.gov. We're trying to move to automated ecosystem where there's automated processing for creating, sharing and assessing as well as reviewing authorization packages and helping make sure that those authorization packages are digital, authorization packages that move through the ecosystem via APIs rather than large document based artifact. We want to make sure our reviews and thoughtful and applicable and looking at places where we can streamline reviews where other agencies have demonstrated high quality assessments and reviews.

And then we want to better support reuse of authorization packages. In part through leveraging the automation but also facilitating adoption assets that can help an agency looking to leverage a new package, build on from the security and the delivery perspective faster.

Next slide, please.

And really we're trying to drive this through one FedRAMP authorization and increasing reuse. So within the memo we outline multiple authorization pass within the new FedRAMP authorization construct. In particular, we're continuing with agency authorizations, but these authorizations are now allowed to be either single agency or multiple agencies authorizations. We have introduced a concept of program authorization, run by Pete's team, the FedRAMP granting an authorization for this. We've also introduced the notion that the FedRAMP board over the course and life of the memo may find new opportunities for authorization paths. We want to support that creativity and novelty that may arise in the life of this memo to support the creation with the approval of the board of an additional authorization path.

I touched on this a bit. But just want to highlight driving reuse through the presumption of adequacy. This means that the controls and assessments, documented within the FedRAMP authorization should be presumed adequate within reuse and we see this as an all-stakeholder approach to get there. In particular we know that we need initial assessments to really meet standard of quality so that others can feel comfortable with that presumption and making sure that there's an expectation within the agency that when they see an artifact within an authorization package that they presume those adequate. We introduced procedures with the memorandum how when the agency identifies the package that might-- how they can respond that back to the FedRAMP team to address those deficiencies.

We also believe if terms of increasing federal authorizations that we need to look at what a lot of our commercial cloud offerings are doing, which is leveraging existing external security frameworks where possible. In particular, we're looking at systems where there will be a low impact level but where FedRAMP authorization may take advantage of existing work or in some cases implementations to achieve a FedRAMP authorization.

And finally, digging a little bit more into the notion of the digital authorization package. As we mentioned, the memo outlines leveraging the open control protocol developed by NIST, to be able to submit note thought as well as transmit digital authorization packages both to the FedRAMP PMO and to agencies. We introduced an agency requirement that within I believe two years, agencies will need to be able to both produce and ingest OSCAL digital passages so we can move to the future where this automation is part and foundational to managing the federal FedRAMP ecosystem.

And with that, I want to thank you all and I believe open it up for questions.

>> All right.

>> We are going to go ahead directly into FedRAMP response.

>> Okay. I'm so sorry. Go ahead.

>> No. No. Apologies. But with that, I would like to welcome Pete Waterman back to the floor so that we can have him go through as the new director of FedRAMP to talk about FedRAMP's reaction to the memo and its impact. Pete.

>> Pete: Fantastic. So as I'm sure everyone knows, everybody had a draft version of this memo well in advance. Ride? Obviously we've been doing a lot of work, preparing for what the real memo would be like. That includes beginning and taking a number of actions to set us up for success when that memo comes out. I'm not going to go through all of them in detail. I think our roadmap is pretty well published and looking forward to updating people on that.

But the key thing related to that is as, Laura mentioned, program authorization. And that memo gives us the directive to develop the federal authorization path. That is something we are leaning into. The process of developing such a new path is complex. And requires a lot of stakeholder alignment. We'll be working through that and sharing. It's all in the process put on us, various policies, laws, et cetera to communicate with the appropriate folks on that as we move forward.

We've also established the FedRAMP board. If you follow the blog you've seen that. We had another big all day meeting last week with cool stuff. We're hoping over the coming weeks, we'll be releasing guidance and incentives from the board on some of those knowledge be a folks interpret and execute some of the responsibilities related to FedRAMP. You can go ahead move to the next slide.

One thing obviously is we increased our technical capacity. The FedRAMP team involves a lot of people. And on the fed side we staffed up in a way that's unusual for a federal team.

I know it's difficult. You know, informally sort of I'll indicate I knew I was going to have this job in May. And I didn't start until the end of augment that is considered incredibly, incredibly I can request. Everything about that hiring process was quick because I worked at GSA a year ago. We have done a lot to get this as quick as possible and build up this capacity.

We also are sending out to a few of our partners over the next week or two, notification that they have been selected for an agile delivery pilot around significant change request. That's the first round of people. We will be rolling more in and reporting on that as it goes forward. And of course, the work, you know, going back to my rant earlier in the meeting, automate.FedRAMP.gov is one of-- establish file interaction with our community who amplified that how we can do it better.

I am-- start doing that out of involvement beyond just code and into some other aspects of the way we do work. I'm excited about that and OMB memo let's us do all that and direct people to support us and help us do it which is super exciting.

I think that's the last slide. Is that right?

There you go. Thank you so much. We're just very excited to finally have that memo and execute towards it. As always, I'll gently remind my community relating to my thing earlier, just because Olympics puts out a memo saying we have to do something, the act of turning our ship is complex. And it takes a while. We're working closely with OMB to do that. It doesn't mean we get to immediately do all the stuff day one. We have working towards it. That is our North Star. Thank you.

>> (audio breaking up).

Now move straight into our committee Q&A where I'll ask members to as a their hands during that time I will call on you to unmute yourself and ask questions. We have a hard stop at 1:15 for this agenda item.

With that, do we have any questions? Bill, go ahead and ask your question.

>> Hi, everybody. First off, Pete wonderful to have you in that seat. I could not have been more ecstatic to have you sitting there. Wonderful to have you in federal service. I have all the confidence you doing an excellent job.

First off, great to have you here.

Second, Ashley and Laura, how's it going? Long time no see. We're often reverse sides on the desk here but cool to have you all. Super wonderful. I think that the new memo has wonderful things in there. I appreciated you taking so much of the positive feedback from the community and from this committee into account there.

And I think it's a radical improvement from where we were. Love to see the acceleration of the automation, that you heard me preaching about for six years now. So all good things on that front.

But the one thing that you know I have to talk about. And I'm sorry but it's a public forum. We have to talk about it and that's the exception process. I was extremely disappointed that OMB ignored the advise of this committee on the exception process. For those in the audience who don't know what I'm Talk&Typing about, federal used to tell OMB that for whatever reason we're using a cloud base tool and can't take it to the FedRAMP authorization process at this time. And as a result we're using it because we need it to fill a critical aspect of our mission. It was a way around that. In the new memo there is a limited series of categories of exemptions. It's tiny, very narrow.

And so that presents a big problem for a lot of us. First and foremost I've commented in this forum before, this puts a bunch of small businesses at a significant disadvantage. We have new comments that came in on this topic. Not everyone as a small business can afford to take their business in the FedRAMP process. They don't have the money and guaranteed other side of this of people wanting to buy it on day one. There are Federal Agencies that do. This doesn't fit into your exemption can bees.

Large businesses have the same problem. There are a lot of new tools that the cloud providers are putting out. To reiterate when I was running OPs, we leaned on that heavily to be able to achieve our mission in the time of the pandemic. There wasn't another way to do that and didn't have nine months for an authorization to come through. The third piece which again I know I'm a small agency, we don't have the kind of budget to take something to the FedRAMP authorization process. And we need these tools to execute our mission. It's critical that we have this. And we have no path forward here as a result.

So I was very curious as to what OMB is advise is to those of us falling into these categories. How are we expected to proceed given there's though way forward for us. And these are tools we're using today. This is something that's currently a problem in the environment I personally run. How are we supposed to proceed forward here? I want to reiterate, you're doing a great job. I know how tough it is to make policy. I know there's inherent cynicism that people are going to game the system. I get that. I appreciate the position you're in. I need to know how are we supposed to move forward here?

>> Yeah, thanks. And appreciate you sharing this. I know you shared this feedback before. Great to hear from you.

I think first we start out with the notion and the intent of the NDA and the FedRAMP Authorization Act which cites that task OMB with issuing guidance which includes requirements to obtain a FedRAMP operation when operating a Cloud computing product or service as defined within the scope.

>> and so part of the our key and one of the really thoughtful conversations we had throughout the development of this memo is making sure that the scope was appropriate and one of the things we found in the process in navigating that was actually, you know, looking at the intent of the legislation and how broad the scope really would be with that.

And so we tried as best we could to balance that scope. So the reflection of what you see the scope is really with all the public comment, with all the additional review and as well as a lot of agency input and great feedback from the FSCAC is a result of the conversations to match the intent of the legislation as well as the policy requirements and input we received.

So within that you see exemptions within the scope. And in particular we also do realize that there's novelty in there. And one of the things that the prior memo did was allow that to be an agency determination really whether or not there was an exemption. One of the things we included is shifted that responsibility over to the newly created FedRAMP board. So in particular, we're looking at it to be categorical any with that the FedRAMP board can then receive requests, this is a category of Cloud Services we believe will be out of scope for that. We encourage you, for the Cloud Services you believe that might not meet that, work with the board and engage with the board around how you might sort of say this is why we believe this will be an additional exemption. So that is sort of first and foremost.

In terms of the additional sort of path forward, we have also included, it's not an immediate thing. Right? We included wanting to have that really on road to FedRAMP especially for the small businesses. We know as an agency, when you're starting to explore capability, immediately saying, you have a FedRAMP. Can deter agencies from moving forward and can be a detractor for the CSPs themselves. So in particular we've created that, we allow Federal Agencies to pile it, new Cloud Services that don't yet have FedRAMP authorization where in the memo we tasked FedRAMP to develop procedures for time specific temporary authorizations in which you'd be able to really take the first twelve months to say, is this a product we'd like to move through FedRAMP. And move through FedRAMP with the expectation consistent with the overall, if it's in scope to move forward with the authorization.

And finally one of the things as part of that, as we move forward is, is really how can we look at reducing the time and cost for low services? Right? Looking at automation, leveraging better reciprocity. And leveraging where we might FedRAMP tailor to support for where appropriate to be making a more flexible process as appropriate for those CSPs. That's high level what I would recommend to agencies faced with what you shared with us today.

>> I really appreciate that feedback. I think you put a lot of thought into this. I think that's insufficient for the reality of what we're dealing within the market today. The categorical base system that you're using is anti-competitive. Because it means rather than saying swath of products is basically exempt and that means the big competitors in the market you're not going to exempt them because they have gone through. These other products that are similar coming from smaller vendors can't compete with the larger market. The other problem, we don't have that funding not in the next couple of budget years looking at how grim things are. We have to sit around and wait for another agency go through it or find another round here.

I'm not going to Filibuster the rest. I would urge OMB to going was accounts reconsider the evidence and information that was put forward by this committee in the public comment period and revise this. This is anti-competitive to a lot of businesses and small agencies. That's a real problem in us achieving our mission.

>> Appreciate your feedback.

>> You all are great and awesome. Sorry I had to say this out loud.

>> Kayla: I wanted to add, in just noticing that, if we're talking about organization, I did a quick count in the marketplace, from the marketplace, it looks like there are eight out of 494 entries in products in the marketplace that are low impact. And there's probably more outside of that. That's what I was doing a quick search for.

I realize that does provide a good scope, a small scope to start with for some of these things. But that might not be the most-- like I could see how moving to LSS might help for those efforts to work through from the sheer shies there are eight. Most of the conversations I have with people,s it's like, why LI SaaS you should do moderate. Just from a pure numbers perspective, I thought I should raise that.

>> Partly I think that's a reflection owl many barriers there have been. And in part of what of the things we're hoping to do is incentivize where it makes sense to move up to LL SaaS. One thing noted within the memorandum is that, agencies can take, can always up lift a package if there's a package. They can take that and add additional controls within their own authorization. You can take a moderate in ATO, work with the CSP to ATO it to high. We reviewed that as broader programming. Conversation is a spring board so additional work once you get there, you can go to moderate as appropriate. Either starting with the agency and potentially that could be facilitate your event jump over to FedRAMP moderate appreciate that reflection and hopefully that is a reflection of how things have been and helping support us in the incentives we can build in this new memorandum.

>> Great. Thank you. Do any of our committee members have any questions for either OMB or FedRAMP?

>> This is Matt from NIST. I'll jump in from a small one. There was a small issue, not an issue, an ad in the assessing security postures around red teaming. Assessments will include reviewing documentation in May also involve intensive expert led red team assessment at any point following the authorization process.

Were there thoughts on when that May also involved be triggered or what would be the offense that trigger that May. And how the results from a red team may or may not be included in the assessment, the authorization or the continuation of an authorization? I'm curious as to what kind of the concept of the use or the, when that may become active in a red team activity.

>> That's a fantastic question. I can speak to the intent of the red teaming expectations. I think one of the things we want to make sure as an objective as we move to really validating the security authorization or security practices present within the CSP is we want to make sure that it reflects as operating production systems. And we want to make sure we're validating the complex architectures in C2 effectively.

So we want to make sure in the course of the assessment, as well as following an assessment and following the issuing an authorization that there's really the FedRAMP team can attest to the real-world security of that CSP.

Regarding the specific procedures and some of the questions you have of when that might occur, you know, going forward, GSA, the board, and CISA will be operating in order to understand and set guidance and requirements and when that might happen. I also note within the memorandum we've created the concept of special reviews. And the intent there is if there is a novel security vulnerability or novel broad threat within the federal enterprise that we want to make sure FedRAMP can do the due diligence from the cybersecurity perspective to mitigate the risk and due diligence of forensic understanding and incident response of those events within the CSP that's authorized.

>> So still I may be TBDs on who provides that expert red team is it the 3PAO, CISA or you know, flushing what experts mean or doesn't mean to make it applicable. Is that work to be specified.

>> It's worth noting that the Director will draw the technical expertise within the Federal Government as necessary. And along with that, as the FSCAC as these conversations proceed we encourage the FSCAC to provide thoughts that you all have in terms of making sure that this is successful.

>> Thanks. Okay.

>> Great. Kayla, you have another question?

>> Yes, I do. So I'm curious how the reaction has been for your office from a Federal Agency's in the topic of the presumptive adequacy. I believe that is one of the big changes for this new memo. And I've heard a lot of conversation around it's going to be a journey for sure for Federal Agencies to be comfortable with this. I was wondering if you guys had any stories or insights or general categories of how the reactions you've heard from agencies here. and I hope we get to talk about this a little bit as a committee later on today, too. I figured for the guests we have here, I'd love that.

>> I'll share, you know, there are agencies we're already approaching FedRAMP with this. I heard FedRAMP has a strong brand. And this is how we approach authorizations. I've heard some folks, a lot of the conversations are clarity within the package review and the expectations. We're having a lot of conversations about how we better clarify that for agencies because the notion, tactically, there is a lot of diversity right now in one agency's issues think ATOs and we understand it's on us to better provide that clarity for where they're not sure they're getting it.

I would say we've also seen a lot of enthusiasm for validating some of the approaches that have been present within agencies.

>> And Kayla, I love that question. It's something we're being practical here at OMB and working with the FedRAMP team. We're connecting agency roadshows. We've done quite a few thus far, have more lined up. Those forms are in the right spot where they're asking questions and kind of going through the memo like we did today. And so yeah, presumption of adequacy has been one. We've been working closely with the FedRAMP team. The way I look at it is building trust in all the products that have achieved FedRAMP, though, maintain that FedRAMP authorization so we can scale and drive home that reuse factor.

That reuse factor and agencies that use many principle is really that magic. One of the many magic positions that FedRAMP or agencies can reuse the materials that have already been developed that have been included in FedRAMP marketplace quickly to issue their reciprocal agencies. A great question and great topic we're continuing to work on, getting information from actions and working with closely with the FedRAMP PMO on-- [NO AUDIO].

So thank you.

>> Can I jump in on that real quick? I apologize, I want to--

>> This is Matt from NIST.

>> Thank you, Larry. This is Matt from NIST. Thanks, Larry. You know, like all good committees, I'm going to say what Ashley said and say it again.

Yeah, I mean, my understanding at the start of FedRAMP when this was getting put together was this is the intent of the program is to have this presumption of adequacy and reciprocal amount TO to enable to scale the agency. Anything and everything that OMB can put on paper and memo as policy to assist with agencies and acceptance of and easy of their kind of business compliance risk concerns that allows them to accept and conduct a presumption of adequacy of another ATO is excellent. One of the things in the email is, presumption of adequacy but this does not absolve of responsibilities. Resume adequacy but you're responsible, the same paragraph of the memo. Anything OMB can do to say, presumption of adequacy also meets your compliance and business risk needs as those department heads would also really help with that reciprocal ATO as well.

>> Thanks, Matt, appreciate the feedback and sentiment the as well. Thank you.

>> Anyone else from the committee? (audio breaking up).

>> I think Michelle closed it up from our end. Many thanks from the committee for your time. And appreciate the opportunity to brief you all today and turning it over to Laura for closing remarks.

>> Laura: You will believing know how to find us. We really believe that this should be a continued partnership and grateful for the work that you are doing and work you're doing in terms of getting this memo here. Please continue to stay engaged and thank you for having us today and giving us this opportunity.

>> Thank you. I appreciate (audio breaking up)

>> Michelle-- no think it's just me. We're having a hard time with your audio.

>> I'm sorry about that. Is this better?

>> Larry: That's a little better. Thanks.

>> All right. Great. We are ready for our break. We will take a 15 minute break. Please be back by 1:30 for us to reconvene.

>> (BREAK)

>>

>>

>> Welcome back from break. We will move onto our first panel discussion for today. We have Jim McCartney from global telehealth services. Brian DaSilva from Mark 43 and Tom Suder from ATARC who are here to talk about their experiences and challenges in the FedRAMP authorization process.

With like I would like to go ahead and hand it over to the team. As our-- as in our previous panels, this is a panel designed to be less formal and more conversational. We have asked our speakers to respond to guiding questions about their experience working with FedRAMP. Committee members are invite today ask questions they may have to these industry representatives during the conversation by raising the hand. And I will call everyone in the order of when they raised their hand. Anyone have any questions before we start? All right. Great. With that, SCRIM, Brian and Tom. Feel free to turn on your video. Would any one of you want to kick us off by starting to shaver how your experience has been working with FedRAMP? I nominate James.

>> Jim: Thanks, Tom. We were authorized in July. But you know, I've heard a lot of conversations around the process. And I think to understand some of our perspective, it helps me give you a rundown of what our path was getting to FedRAMP authorized.

Because we found just about every loophole and crack you can fall through in the process. So we were approached by a company-- the company was approached by VA at the start of the pandemic, something they wanted us to go through to be used in facility.S there was a naive thought that it could be sped up and gone through quickly. Fact that we authorized in July says that it didn't happen that way.

We did not, the company did not get an APO help us. The consulting side we did ourselves and we successfully completed our first assessment with both the RAR and SAR in August of '21. They were submitted to it. When we went to submit it on, when they submitted it all, the PMO said, said we want the RAR we don't want to see the SAR until you have the agency ATF. We got the RAR review in December of '21. Took us until June of 2022 to get our ATO. And we got put on the list to go through our SAR review by September of '22. At that point they said it who's four to six weeks. We had the SAR review in December of '22. All the work we had done on the RAR review, none of that got incorporate because we did if all at the same time. By the SAR review, the law had changed. Additionally we had changes we wanted to make but we were told you can't make any changes until after you finish your SAR review.

We're sitting-- we get to the SAR review and they said, it's a long time since your assessment, you need to go through another full assessment. I said, okay. We then-- but then because we weren't technically in the FedRAMP program, even though we had moved in processing, but then-- we also fell off the markets place because outside of-- we had no control of that.

But we then went back, got the significant change approved by the agency, went through it but under tremendous pressure doing another assessment. We were still initiating our change as we did our assessments. But that got done in August of submitted in November of 2023. We didn't get, go through the process, then we have three SAR review meetings to finally get approved in July of '24. We had another significant change trying to get approved. It's been a challenge. But I will say I don't begrudge any of it because the way I look at it is, you know, offering our product needs to be as, our commitment has to be the same level as any Federal Agency.

One of my experiences is I helped write a business continuity plan for Jenny May. And this is after the housing bubble. And they were sensitive about making sure they were doing their job. So thinking of, the way I now think about it, is the way our solution is being offered, it's being offered the same way making a payment on the MBS account is the full credit of the United States. If you don't come at it to play it at that level and respect, you don't belong coming to play in the FedRAMP space because that is what has to be delivered for the Federal Government and the services.

I said a lot. I'll turn it to Brian because he had challenges he dealt with. I want to start with that.

>> Brian: Thanks, James. My experience was a little different. We were quicker to get overall authorized back in May of just a few months ago in May.

Overall it's a working with the FedRAMP during that process was touch and go in terms of challenges, in terms of the expectations from the-- we did hire a consulting company or a three-- consult us through this program, help build it, help us consult through it in order to get us to the point where we were ready to go in fronted of a three panel in that initial assessment and the PMO review.

My feeling is by the time we got to the PMO review, we did our first initial review, it was very evident that they were still a very big disconnect between what the 3PAOs are assessing us on, even though it was eight months earlier versus what the PMO is expecting us to deliver. And so we just had, we had a number of findings I couldn't imagine after having a consulting company come and we paid them to help us get to the point where our documentation is up to the adequacy that the FedRAMP expects, then the 3PAO assesses us, help us get to the point where we needed to be assessed and get what we needed to get the ATO.

The time the PMO reviewed it, it seemed there there's was a disconnect. How many findings we had. For me it was hard to see how far the gap was. In my mind, and I don't really what bullet point to hit this time, that's where I would see my hopes and dream where the 3PAO assesses you the same level as the PMO. That review should be exactly what the PMO should be expecting to look at in my mind. And the PMO is validating to that level of degree but there shouldn't be that much of a disconnect. I'll turn it to Tom for his thoughts.

>> Tom this. Thanks, gentlemen. I actually would like to ask 3W0EG9 of you a question. Can you imagine a world if we didn't have FedRAMP? What would it mean to your companies if there wasn't a program like this. What if every agency did your their own thing? How would that affect your business?

>> So in some ways it might have been easier. We were asked a number of times by the VA if we would just-- satisfy's like, our life would be easier if you put an intrans of your platform inside our data centers. Our answer is that's great and it helps you but we couldn't do that and work within I other Federal Agency. We made a conscious choice that FedRAMP was absolutely the way to go because of what we're trying to do and where we're trying to go.

>> Great. Brian?

>> Brian: Yeah. I mean, I would want-- we have an environment that's not federal for our state and local agencies. And you know, we hold ourselves to a level of standard. So I would expect us to follow the same level of standard, have some baseline using NIST, NIST as a framework in order to provide kind of that attestation or compliance that meet the needs of the agency is looking for.

And certainly, I think it's kind of, once you do that once, the whole point is to test once, comply many in allow agencies to be able to use your products as what FedRAMP intends to do. Create that central repository of hey, they meet this need. You can have guarantee or certainty that they meet all the expected controls. But I still feel, double tapping off of that, I still feel there's a disconnect again in terms of talking-- now we're authorized and getting into the weeds with agencies who want to use our product, who want to buy our product. And it still seems we're FedRAMP high authorized and talking to some large agencies. And they still don't understand how a high environment can have everything. One very, very large agency came to us and says, we see that you're high. But we want you to build a moderate environment, separately. And we said, why? Why-- wouldn't you want the more secure environment, the high environment? And they thought they were taking on more risk by being in a high environment even though they're going to issue an ATO at the moderate level.

So that's just, and that's not the only time we've had the conversation with an agency around their confusion on what they need to do, they need to-- or how to use our product and use FedRAMP to their advantage.

>> Great. Great. For those who don't know me, I'm Tom. We bring government industry and academia together to solve problems like Cloud security. And unlike these two soldiers on the frontlines, I think we're more of the-- if you equate it to the California gold rush, we're supplying the pick axles and shovels. My experience with FedRAMP from the beginning, I got approached by David, he had on his team. Maria wrote, sunny-- Paul, among others, it was a superstar team, I think the idea was he have, very sound. And I think it's been overall great for the DoD and civilian agencies.

I think as we've gonna long, I've seen trends. I see a lot of company is, almost major companies on FedRAMP is a member or has done work with us. I almost feel sorry. We don't talk business enough. But I almost feel sorry for the first team coming in that is getting FedRAMP or trying to talk to the President of their company. We really need this FedRAMP. It's going to take longer than they think. It's very, very expensive. By the time they get the FedRAMP authorization, a lot of times the team has lost their job. It's seduces a lot of costs. We really need to think of taking the costs out. We looked at OSCAL, I don't know if we really implements that to the fullest extent.

You know, it is, I think we need to break down every aspect. I know ATARC. The ATO process for the agency, it's long. FedRAMP is a subset of that. Why is it taking so long? We need to ask for more resources.

Through the years, a lot of, I would ask the PMO why don't you ask for more resources? They took it as a badge of honor that we worked super hard. If you have more resources you wouldn't do so much cost for the companies because we have shorter terms. These gentlemen discussed the problem to quite an extent. I don't want to cover that. The 3PAO program needs to be looked at. I saw that from the beginning I saw that with 3PAOs. You want to keep a diversity of suppliers. I think a lot of the vendors don't have that. You're stuck with it, with self of them that won't be named. They can pick their price.

And I think that how much it's going to cost upfront ends up being a lot more almost in every single case. Continue working with agencies, for FedRAMP that might cover what you need. I was talking to the vendor the other day, we got through FedRAMP. This is fantastic. You have another year to get the ATO now because the FedRAMP controls aren't enough and it's a whole convoluted process. The FedRAMP PMO has to work with the other agencies. What do you need more than FedRAMP?

I think a consideration, it's good to see metrics, how much does it cost these companies? What can we do to make it easier to get the world class technicals used by the Federal Government? I see it in DoD all the time. It's impossible to bring the Silicon Valley companies. It's difficult to bring it in defense in particular. It's like that in a lot of agencies. How can we really bring the software, the idea is to get the software through fast and safely and make sure it has the right security controls. I think we need to be moving to that.

That's some of the things I've seen. I worked with 250 and 300 companies that dabbled with FedRAMP. You don't know what FedRAMP is. You're not ready. That's like the bar. You at least have to have something about FedRAMP in place to even do business with the Federal Government.

>> Tom, I want to go on that. A couple of things Pete talked about. Pete you did a good job of bringing to light some of the issues that frankly very few people, certainly not in Silicon Valley most people in the commercial side don't get. What are the constraints in FedRAMP and limits and how quickly they can move.

Laura talked about OMB trying to move this faster. It's still going on government speed. Unfortunately there's a reason for that and it's valid. And as much as it's nice to make it easier and simpler, at some measure you have to respond, working with the government. I think its was the March meeting when somebody from OMB said, working with the Federal Government is not for the faint of heart. There's so much truth in that.

For me it's like how do we work within the constraints with what FedRAMP or the agencies or the 3PAO can allow us to do?

Like we were talking yesterday, what are the challenges? What do we see in the marketplace in one of the biggest things, the biggest thing I see as a challenge is there aren't enough people to play at this level who can really play at this level in a way that actually is enabling. Brian we were talking about, the first you hired the consultants. The first people they put on the project were good and progressively went to newer people. They weren't getting you up to speed to be able to step into your assessment.

And the question that I would love to hear from Pete at some point, you said, bringing on a whole bunch of people. And Tom you talked about it. You're bringing a whole bunch of people. What programs are you putting in place to grow the people so they can participate at a common level? I want to knows what that looks like because I want to do the same thing. I want to find ways to grow people.

And to be fair, a lot of people think they can may at the level. This is the show. A lot of people think they can play at that level and that doesn't mean they necessarily can. But that's one of the biggest issues I have. But one of the pain points that I wanted to, a couple of pain points I want to talk on, the number one thing is the consistency of guidance. Twin my three SAR review meetings. I had one person give me guidance, specific one, the second meeting, I did that work. When it came time to the third meeting, they're like, what is this? I said, I did exactly what you asked me to do in why did you do that? Because you old me to do it.

And that is concerning. And yes, at some point we need to get to the knowledge base where the to go could be out. But in terms of suggestion what might be helpful for communications is, if there was a forum where 3PAOs and CSPs can openly communicate about some of the issues and come to resolution to where it could be handed to the PMO or the PMO can then actually weigh in, speaking as the Federal Government and put that guidance out, that might be a way to move it faster.

And I will say all the things I'm looking at in thinking of improvements are very shawl because I think you guys have the big issues, that's fine. Where I can help where we can be of use is in the smaller areas to streamline it.

And I guess one other area that came up, mostly on March 28 meeting with the 3PAOs is a conversation about moving towards centralizing continuous monitoring. I think it's great. But it is definitely incongruous with the 3PAOs and PMO were which is we accept no responsibility for any risk. That's up to the agency.

Well, if you're going to do centralized-- by definition, you're accepting the risk for that agency for the continuous monitoring and the actions on it. I suggest the actions perceived-- dealing with risks made the process harder. For example we have a couple of external services that were reviewed as not having any sensitive data. Completely sanitized. I now have them on my-- because even though I'm under agency ATO I'm allowed to use the non-authorized services, I have to have it on my-- because it's a standard.

So there's a disconnect that I would love to see somebody take a look how to address. But the other comment at the beginning talking about the number of people getting into the 3PAO. It's my understanding that increasingly, CMAC will use 3PAOs. If there aren't enough people to do it. Now, I'm in the program. I think the PMO doesn't always do well distinguishing between somebody's first time through and a repeat. And might be easier-- having some consideration somebody going through the first time might be helpful to have that conversation look a little different. Brian, I'm sorry I talked a lot.

>> Brian: No, I think you hit a lot of the same points I would bring up in terms of the consistency of the messaging. We went through our first meeting with the PMO. They found dozens of findings which were concerning. And the second review, one of the things we haven't talked about really are the things that worked well.

The overall organization and structure of the PMO's ability when they start the review process and have discussions, I would say that worked really well. We knew when we were going to meetings how often. They were up font about it. So I will say it was nice to get that kind of right off the bat in terms of just knowing, hey, while I think three weeks is too long to go over these issues, it was nice to know we're going to meet in three weeks about our next meeting.

But when we went to the first one, we had issues. Great. We went to the next one, we talked about those issues that James mentioned. But then it was, hey we also found these things now. And so it was, why didn't you find them if the first review? Because now we just lost one meeting to go through these new findings initially. And so now we have one more meeting to kind of get through everything. But in essence we only have one meeting to get through of those identified in the second review, if that makes sense.

So it really limited us, our ability to make sure that now we're trying to capture things that were found in the first review. By the second one, now we only have one more meeting to capture things that were found in the first and now the second. So we just didn't have a lot of time to address those issues and it was really the inconsistency of the review from the first. It just seems like it's unfair-- I know you guys have to find the issues. And we want to fix them. But it's either more time needs to be spent on the initial review so when we go into the second one there is isn't additional new findings we're told. That kind of changes our resources, changes our timing and impact of what we're trying to prioritize on which ones we need to fix first, second or third. I would say that was one of the pain points we found.

>> You keep going back and they keep I can canning the football away from you a little bit.

>> I mean, we can keep talking but does anybody have questions for us to start?

>> Carlton Harris here. I have a quick question for you. In the recent release of the modern-- sorry. In the recent memorandum that was released, is there anything in there that would have helped you in your process with some of the troubles that you were seeing going through it?

>> I mean, I haven't read through it yet. I've been focused on other things, like getting our significant change approach. But-- I was not, I did not struggle with what the requirements were how to do it. Franks lit a lot of it was growing the team to play at that level. And then frankly a lot of it is documentation and making sure that it's appropriate, making sure that we're answering the questions that we needed to.

And a lot of it was time. Really was the time to get, getting through, getting assessment. It just took a lot of time.

>> [NO AUDIO]

>> A few hands. I think we're--

>> You want me to call on people?

>> I think she's disconnected there.

>> (audio breaking up). Please go ahead.

>> Michelle, you're a little bubbly in your audio there. I'm not sure who you're--

>> (audio breaking up) yes, I'm calling on you, Matt. Go ahead.

>> Thank you. I have so many questions. Most of them around my ignorance. Please be patient with me.

Tracking on a lot of the pronouns being used.

>> I apologize.

>> Again I think a lot of it is you all are very experienced in going through the meat grinder. Whereas I'm looking at it from the outside.

So you have your 3PAO assessment and then there's, every now and then there's talk about either second assessment, second review or another review. And I'm trying to understand, if and how much owns rework is being done after a 3 PAO assessment is then delivered to an authorizing official or PMO which ideally is just-- is it complete to a level of risk. Or is there a reassessment and return? I'm trying to understand how much trust extension is being given to the 3 PAOs to do their job and do it adequately versus really a double check on and a need for having stronger trust with what the 3 PAOs do.

>> It absolutely makes sense. And so I can speak to it from a--

So one by the time we got our first SAR review it had been a year and a half since it was accomplished. It's been too long, you need to go through a full initial assessment.

>> And they did that by time and not necessarily by technology change?

>> We hadn't changed the technology at all. It's been too long, go through it again.

>> And by they--

>> The PMO, the FedRAMP PMO said we are not accepting this because it's been too long even though there was nothing on us. No part of it was our fault. But we said, okay. Depend, I don't control the ball.

>> I understand.

>> We made the change. We went through another assessment with another 3 PAO. Submitted it, and we were told towards the top of the list, it still took from November until February before we even had one. And it was May and July before it was even-- before we had our session. And we had three different meetings from the PMO to go over aspects of it.

To your point is, was the PMO looking and judging and assessing whether the 3 PAO did a good job and absolutely. But they were also looking at things they didn't understand about our platform. And they needed clarification on.

So part of it was their education. But do I think they do a lot of rework? Yes. I also think they are -- the PMO is not necessarily as consistent with their guidance as they could be. And they often times in the SAR review will be holding us to standards or guidance that wasn't the case when we actually did the assessment.

>> Okay.

>> So you know, and-- and to a certain extent, I don't mind that as long as they're not going to stop me because they're looking at it at where I need to go in the future. I look at it as things I need to do to have my system be better.

>> And I think one of the things you were talking about as a open, common sharing platform to have these discussions, set precedent understand implementation guidance for 3 PAOs and CSPs so that you can establish repeatability, understandability and know where those bars are to some extent.

That's-- okay.

>> And I do think it will be better if the PMO, they could look in you about the PMO, unless they felt necessary wasn't weighing in. As Pete talked about, when someone from the PMO puts something out, that is now official government guidance. And there are all sorts of constraints on that, that not only understand, I appreciate.

But if we can take what happened in our assessment and bring it to other CPT SP or 3 PAOs, we can get some sort of consolidation around it and bring it back to the PMO and say, here's kind of what our thoughts were. And that can be more of a conversation rather than official guidance.

>> All right. I have one more question that I want to jump on before Bill jumps it. That's a reciprocity discussion in the memo. Do others outside the Federal Government look at the FedRAMP-- are you able to use it with folks outside of the feds? Are there other frameworks that you implement that may or may not be put into that reciprocity bucket for the future like cloud security alliance or ISO or GDPR or anything else?

>> Sure. We have not bothered to get any of the others. As far as I'm concerned, FedRAMP is gold star. The one thing I would say is GPR because that's a privacy regime not a security regime. So those are fundamentally different. But I don't look at those-- and this goes to something talked about in a previous meeting, looking at reciprocity between FedRAMP and SAR. The depth that have to be there for FedRAMP blow away any kind of SOC documentation. Does that answer your question?

>> It does. Thank you, James.

>> B,o, you're next.

>> James, Brian, Tom I appreciate your feedback here. It's incredibly rich and some of these hard truths are folks actively have to hear openly and publicly in a way to go over through and acknowledge.

I will tell you, having sponsored 30 different cloud of service providers, big and smalls, including Colin from-- that spoke earlier during the actual public session, this is not easy. It is hard.

There are multiple stakeholders, multiple workstreams, and I think there is sunlight at the end of this, I think. All that is to say there is broad commitment to effectively acknowledge that there are challenge gaps. There are work stream gaps between OMB and PMO. And the FedRAMP board. All of this is essentially coming to a head in terms of being able to put real actionable recommendations that are, can be implemented to help to go through, perhaps not directly ameliorate the challenges you went through but hopefully make it streamline and every other provider that has yet to really experience the opportunity and the challenges that come along with FedRAMP.

But I think the feedback here is absolutely welcomed. But there is, I think this broad acknowledgment, and there is ideation how to effectively look at the broad work of streams across 3 PAO, PMO, as well as leveraging organizations that effectively have, in some cases different understandings, different expectations what adequacy typically looks like.

I think there is an answer that we're coalescing around. And I'm hoping that, a year from now we're going to be better than where we are today.

>> Yep. Thanks, Bo. I'm hoping that somewhat what you're saying, is because you know you can't. One of the things, towards the end, you're talking about, something that goes back to what Laura said at the beginning. Doing road shows.

One of my greatest challenges working within the agency we work with is a lack of understanding of what it means to differentiation between having an ATO or being FedRAMP authorized. And what that means and doesn't mean. I think there's not necessarily from the people within OIT, the business side. If that conversation with the agencies can go beyond just the technology team, the CIO shop but up to the people looking for the service to use them, that would be significant benefit to the CSPs because it alleviates the conversation so I don't have to have it and try to educate the agency personnel on.

>> I was at the Mark center, part of the Pentagon extension in Alexandria. I was talking to a general about this. Remember they are rotating in DoD, from artillery to overdoing IT.

Really a limited understanding of FedRAMP, how it fits into the ATO process. There's continuous education, continuous -- I think there should be sessions and just be constantly on the road talking to folks, to educate them and help them adopt FedRAMP.

>> Bill?

>> Bill Hunt: SEC. Thanks, everybody, for the great presentation. Tom, long time. Great to see you, my friend.

>> Your hair is longer.

>> Bill: Getting there. So I have a couple of questions I want to ask you all. Filibustered so much of this session already. I want to go through quickly.

The purpose of today's session is to try to drill down on the recommendations this panel is going to have. There are a couple of area I was noting down.

First off, I will admit my ignorance here. We have heard there are gaps in the service available for the 3 PAO side to do the evaluations. That was relative news to me. I haven't been paying close attention people wait that long to get started in the process.

A few recommendations on what's needed there. Do we need more 3 PAOs? Do we need them, to do more hiring and incentives the government can provide there. Are the assessments too thorough? And around the velocity of the 3 PAOs, what would you suggest?

>> Brian you want to start that one?

>> Brian: It's train the trainers, right? You're coming up with guidance. And you're pushing that guidance down. And then you're hoping that somebody, some 3 PAO, are looking, taking that information, able to undergo and understand and apply it to whatever the CSP is doing. I think they need more because we had conversations with the consulting group who is a 3PAO and actual 3PAO about red teaming or something that's coming out.

And both of these quote and quote 3PAOs didn't have guidance on what the GSA, what the PMO is going to expect. So it's like really? These are top two of the top 3PAOs that were in the industry. And they don't even understand what it's coming out in terms of guidance. We had to go kind of and say, listen, until he with-- we can't do something until we have more guidance because it takes time, money, resources. When do you want us to do this? We're up against the deadline of getting some assessment done. And so we have to say, listen, we have to put this on pause or have to take the risk that we have we're going to get dinged. We know we're going to get dinged because there's not enough guidance. And it's ridiculous I can't rely the top 3PAOs to know what the PMO is expecting.

>> James: For me the answer would come back down to the number of people that can play on this level. The same level Pete is having, how he's growing his team to play. From my perspective, the only way to understand what it means to go through a FedRAMP assessment is to go through a FedRAMP assessment.

I mean, I teach, provide-- re-record all of our sessions to new people we have them watch the sessions to get them have a sense. They're not going to get it until they're under the gun and had to answer the questions from an is assessor. So it's hard-- as people said, this is hard. This is really hard. So a 3 PAO does to grow their team, something similar to what the PL does to try to grow their team, the knowledge of their team. If there's a formula that works, share it. Everybody can use that to how to successfully grow teams of people to play at this level.

Maybe Tom has an idea what a structure might look like to grow the expertise of the people to be able to do that.

Bill, you had a great question, can we offer other incentives? I don't know what other incentives you can offer within the structure of FedRAMP other than, you can go through this. You can get on the list and be used. You have other ideas of incentives, I'd love to hear it.

>> I don't know if government start giving out grants to-- start new 3 PAOs. How do you address the velocity you're seeing?

>> James: The biggest bottleneck that I saw working with a 3 PAO or different PAOs is the biggest hurdle that they have to go through or the PMO has to go through is learning and understanding the system that they're assessing.

That's really really hard. And although our system is small, what it does and how it does it is very come next. To understand the nuance is critical in how we address the controls. I spent the vast majority, the heaviest lift I did with 3 PAOs was educating them on our system.

And you know, I don't know anyway around that because, if you-- for a PAO to successfully assess it, they have to understand how it works and how it fits together. And that-- I don't think you can turn that over to AI. Because that's the understanding that you get to. I don't see a way around that.

>> Brian: One thing to point out. The issue also is the fact of the number of CSPs that have gone through each level of impact. You have so many of the low and you have 3 PAOs that were able to assess a CSP because the number of controls is less, and easy to employ. And then you get tougher, more with the moderate. The number of CSPs. You're in Oracle. There are only a handful, a dozen more actual CSPs at the high level. There's not enough 3 PAOs who have gone through that experience with those CSP. They might versus gone through it ten times with moderates. Numbers don't lie. They have gone through it once or twice with the high. That draws part of the problem is when we went through the high, we didn't have, we didn't have the expertise because they haven't gone through it. I don't not what kind of incentives you have when there isn't-- you can go months without anybody going through the high impact level. You know what I mean.

>> Yeah, that's extremely helpful. I have other questions but I don't want to take everybody's time. I will let my colleagues here jump in as well.

>> Thanks, bill. Go ahead, Kayla.

>> Kayla: So I've heard this a few times from your conversation here. And when we talk about the ecosystem in general not having enough hands on keyboard or even just availability to communicate processes and next steps and stuff, the ecosystem doesn't have enough talent to play at the level. Do we mean just understanding the FedRAMP process? Or are you guys referencing more the security skill set? We don't have enough people who have the technical security know how to handle these FedRAMP conversations? I'd like to understand which perspective, which audience we think really the lack is here.

>> Partially the FedRAMP process but not really. And I'll not even looking specifically at security. I think if you pigeonhole FedRAMP as a security issue, it's missing the point. This is a business process. Yes there are technical aspects to it. But this is-- the reason you're playing this is I have to know my systems so much better than people who don't play at this level. I have to though every last detail for services I'm leveraging from Microsoft. I need to know everything about how they do it and document that effectively. And at a sixth grade level so our 3 PAO can understand it. The PAO when they look at it can understand it easily. That's hard. And that's not about fingers on keyboards.

That's the kind-- that's what I'm talking about. The whole point of FedRAMP from my perspective is to get a good operational product that is secure, resilient, and scalable. There's a security aspect. To me FedRAMP is less about security than it is much more operational and how do you manage your organization.

And to be able to do it at the depth that we do is not easy and most people just aren't willing to put in the work to do that. Does that answer your question?

>> Kayla: It does. It's interesting. I feel like what we heard so far and profess about FedRAMP is that it is the gold standard for security.

>> James: I'll not suggesting it isn't security. A lot of stuff I have to do isn't related to security. It it's compliance and business processes and how mature my process is on how to deal with it. The security is actually the easy part from my perspective.

>> Kayla: Yeah, I sit on the CSP side. I hear that. I appreciate the conversation on that.

>> James: Sure.

>> Michelle: Go ahead, Marcy.

>> This is Marcy. I'm the on the 3 PAO representative on this call. This has been an interesting observation. We spend a lot of time in the trenches with our clients and call service providers going through this entire process. One question I have for you, as you've had varying experiences getting your initial authorization and you're looking, moving through toward annual authorization and through that process or annual assessment, when you kind of had those hurdles, James I know you had to undergo that full initial again basically.

And if I understand the timeline on that, was a lot of that due to the length of time it took the initial agency ATO to get into you the office of FedRAMP queue?

>> That was definitely a part of it. Yes, absolutely that took forever. I won't even deny that. But the fact that we couldn't even submit the SAR to the PMO when it was done but had to wait until the ATO had been granted to me was an issue. It's done. It's there, why can't it be put in there to note that it was done and have it go the same time it's going in?

Again we did not go through the normal process because we it the RAR and SAR at the sale time because we're trying to address a pandemic need. We did not go through the normal process. I get it.

But there was little flexibility on working through that. And recognition of how to do that differently. Does that answer the question?

>> It does. I was trying-- we have encountered a variety of scenarios and many pain points depending no matter what. I was trying to make sure I was understanding the primary issues and hurdles you encountered. So I appreciate that.

>> James: Sure.

>> Tom: One thing I suggested to PMO is how can I have a BPM where the things are in the process so I have security people to do security things. How can I manage this process better so I can focus my security people on security things. And the management is automated. I don't have to go through these cycles going back and forth. There are things you can do to maximize your talent, if that makes sense.

>> Bill's got his hand up still.

>> Bill: Sorry back for another round. So one thing that you touched on, Tom, you brought this up earlier about particularly small businesses showing up and just not being ready. Just trying to stop them in their tracks and say, you don't know enough to even proceed with this.

And this is something I'm extremely sensitive to. Having been a small business owner in the past myself, working for SBA. The small business I've sensitive to. I don't want a free pass for anybody. I have to know that the tools you're using are safe and secure and we should feel safe putting our data in it. At the same time the entry is so high.

So what can we all be doing as the government and again like Tom organizations ATARC how can we work together, close the gaps, so people aren't showing up, on day one and being like, I have no idea what I was supposed to be doing. I haven't done the basic homework. How can we close the gaps aggressively in the government may be providing smalled business incentive grants for security. Do we need to do training? What are outside the box ideas you all have?

>> You want to go, Tom?

>> You go first.

>> James: To a certain extent, it goes back to what Laura said. Which is the government is not used to having to market its rules and organizations and how it does business. The government's the government.

I saw this years ago working with the FTC organizations like ATARC to bring it to the front to them and bring that out and say, guys, this is what it is. This is how it is to do this.

Maybe there are other ways, but maybe other associations that can do that and having people from PMO or 3 PAOs or CSP talk about it would be helpful. Unfortunately the work can't always come from the government to do it. Do I think grants are great idea? Absolutely. How to make that happen is especially for agency your size.

If you can help somebody find a grant to be able to help them go through the process, maybe that's an answer outside of the box way to use existing structures to get what you want for your agency.

>> I think we can provide guidance for them as we're starting out with solution. Here's what you should be doing right now rather than develop a whole solution.

Also are you using some modern architectures like containers? That should probably help you. I'm not into it. I heard it hurts you sometimes. How can you have that, do that? And also like phase III a lot of times they will help you get ATOs, and OTAs and things like that. Sometimes an O TA on the DoD side is to help you get your ATO and give the solution so you can use it.

It's not easy. It's the advice from the beginning. There were organizations that do a wonderful job, helping you in the beginning stages prepare for the ATO. You're trying to develop a product in the beginning not so much getting a customer. You're trying to develop a product. You should keep that in mind. If you're going to do something like FedRAMP that will help you in the financial sector. It's going to help you in other markets you want to get into. If you're thinking security, you'll be much further ahead.

>> Great. One last question for you all, and I will end my tie aid here. The very same vein. The process after the FedRAMP authorization for folks getting in the door, this is still a barrier. I want to applaud again NIST and OMB for their stance on the presumption of adequacy of the FedRAMP assessment. The FedRAMP assessment is only 60% of the control. The 40%, the agency is still speedometer for, the vendor is still responsible for.

Do you have suggestions on how the government can help accelerate that instead of waiting for FedRAMP and ATO process so we can get the tools in the government faster?

>> James: It's a great question. In some measure part of the problem, particularly the small businesses, they have to grow their level of expertise to be able to do more than just build a product that's nice. Again it's all the rest of it around it. At some measure, yes, Bill, you might want a couple of little things for you and your agency.

But the process you have to go through, I was in the military for a while, the same process you go through to buy a hammer is what you do for buying an aircraft career why. The acquisition process is still the acquisition process.

You know, what you want to go through for software that does something nice in there is the same one that goes through for Azure. So I don't know how to do that. I don't know how to suggest for you to do that. And that is part of the challenge. But again, that product has to work no matter what because, one thing that might be interesting to look at, is there a way to differentiate between those products being used within an agency versus those that are being offered to citizens?

So for example, we're being offered have I VA to veterans. That is a different type of service than one you use in your back office to do different things. Maybe there's a way to differentiate that and therefore put a different level of expectation.

I don't know. It's a thought.

>> I'm thinking about tools that might be reused this. I recently had to take a product through the ATO process myself with my team that I think Bo, FedRAMP originally. They've been using for almost a decade now. Figuring out how we can accelerate that reuse part of it.

>> James: Is that more of an acquisition issue or process for ATO? I don't know the answer to that. But I mean, that also comes to mind of the disconnect between the FedRAMP or ATO process and the business owners and the acquisition. There's not necessarily a lot of communication. But I would chuck that more to government bureaucracy and not being able to update the structures to address those issues. I don't know how you get through those. We've-- wherever we could, we shifted or try to give the answer to go take the next steps for us. We do the work to hand them the answers so they can do it for us.

And we took-- we kind of took the steering wheel of the car, what do you feed them next? Can I do present the work for you and now you can take it on? How motivated is the CSP to get through the process? What do they do? The next steps? It's different from agency to agency. At some point that's part of it.

But I had last thought on that, Bill. It comes back to the assumption of risk. Like if you're going to say, hey, FedRAMP is going to absorb, taking on some of the risk assuming some of this risk, that process should become easier because the agency says, that's good enough. That's a difference in mentality from FedRAMP right now which is, we assume no risk. We assume no liability. That's up to the agency.

I think that's a big disconnect that you're trying to deal with how to get the agency ATOs to go faster.

>> That's a constant pain point for me. Assign the risk back to the CIO, depending if you're under the-- FedRAMP can't legally absorb any of that risk for us even if they're doing a lot of the work.

>> There's also some companies out there like the stock commerce of the world. Where they build out a framework for you so you inherent a lot of controls off the bat. I haven't used they will but I've used other companies where they're already ATO'd or whatever. You're an add to their-- there are different approaches. I don't know enough about it how it's worked for companies. It seals like inherited a lot of controls, paying decedent amount and not as much as going through from the beginning.

I want to learn more about that and see how that's affected other companies.

>> Unfortunately we are out of time today for this panel and questions. But thank you, thank you so very much Jim, Brian, and Tom for sharing your experience. We will go ahead and move onto our final panel discussion. Ralph Jones from the Department of Treasury David Meyer from the department of education, and Susan Schultz Searcy from the pension benefit all here to talk to us about the challenges of agencies during the FedRAMP authorization process.

As before we have asked our speakers to respond to guiding questions working for the FedRAMP. Members to ask additional questions they may have to the liaison, by raising your hand. And I will call on everyone in the order your hand was raised. David, Ralph and Susan thank you for joining us. Turn your video on if you like or unmute yourself if you want to respond. Would one of you want to take us off (audio breaking up).

Sharing how your--

>> Sure, this is Ralph Jones from Department of Treasury. I would be happy to start.

>> Go ahead, Ralph.

>> Ralph Jones: First of all, thank you for your invitation to today's meeting. Just for some background, treasury has been working with the FedRAMP since the inception with the original OMB memorandum in 2011. We have positive things to say about the state of the program.

In terms of our experience in working with FedRAMP, the PMO has been very responsive through the authorization process. We have sponsored several CSP via agency ATOs and we have also JAB ATOs as well. We appreciate that FedRAMP has fostered baseline in security expectations around the cloud.

As were a lot of agencies we initially struggled getting confidence around whether these CSPs were able to meet the same NIST controls, hosting a system On-Premise assess. The FedRAMP process has enabled us to gain that assurance and gain confidence in the rigor behind the controls in place.

We also think that the 3 PAO process has worked well even though it has taken a lot longer to go through assessments than I think a lot of us would have envisioned. I certainly can share some of the pain going through some of the initial authorization process that others had mentioned today.

One area where we have had definitely struggles is in figuring out the customer responsibilities when dealing with multiple cloud providers, hosting to go for the same system, for the same authorization boundary.

So we think the customer responsibility matrix is definitely a good start. But as the FedRAMP looked to modernize and go with digital authorization packages, anything that can be done to streamline the customer responsibility process so that agencies know what they're responsible for at the end of the day, I think will dramatically accelerate the ATO process.

Another pain point for us is in continuous monitoring. We found that there isn't as much consistency in the level of reporting between different CSPs as we would like. And when there are deficiencies in the continuous monitoring process, we struggled to figure out how to escalate that appropriately so that those deficiencies can get resolved in a timely manner. In terms of hopes and dreams of the FedRAMP modernization process, the big thing is to make sure that as we look to automate the authorization process and leverage some of the industry frameworks, that we don't forget in that process that at the end of the day, agencies are responsible for ensuring the public trust. So we need to make sure at the end of the day that the security controls we're going to wind up with are going to meet the same high standard that we have today in this 853 revision five.

And the associated baselines in 853B and the current FedRAMP baselines.

The second thing is just to look at ways that we can reduce risk for new CSP. Make sure that if we have somebody new to the marketplace that there's more guidance and more hand holding available to them so they are willing to take the leap of faith in working with the Federal Government. It's challenging to do the work that the government asks CSPs to do. And we don't want people to be scared away as we try to expand the marketplace.

The only other feedback I would provide is just that I think it will be imperative that all agencies work together with the FedRAMP PMO as some of the elements of memorandum 2415 get finalized into policy so that we can iterate and learn as we go along.

For example, as we figure out what types of CSPs are going to be subject to FedRAMP and which are not that we collaborate so that we strike that right balance between making sure the FedRAMP program has solid footing so CSPs will have the leverage to follow it. And making sure we don't box ourselves into a corner and not be able to utilize a cloud product at all because there's just no model in which they can go through FedRAMP authorization. That's pretty much my comments. I would be willing to answer any questions.

>> Susan Schultz Searcy: I can run through my next. We appreciate the opportunity as a small agency to come to the committee and talk through some of the things that we're experiencing. I think it was great for me to hear the CSP perspective. I think sometimes we're in this bubble thing while this process works for the other guy. So we have to deal with it.

But it was nice to hear that they're having some issues that they're working through as well.

So what works well for us right now, a small agency, and with pension guarantee corporation, we have been an agency partner, sponsoring and also a consumer. We do leverage, a good deal of Cloud Services the we recently developed our cloud dashboards that we see clearly what we have and where we have it. We have been very supportive and gotten a lot of support from FedRAMP PMO, on demand support when in the midst of something, being able to reach out to somebody at FedRAMP and ask questions early on so we don't get stuck in the process later on, getting sent back to start. We appreciate everything we've gotten from them.

The guidance policies process that is available to us is great. It has helped us build our own cloud security guidance which encompasses the FedRAMP requirements or agency requirements for being an agency partner or a consumer of cloud. Makes it nice and crystal clear for our agency folks on what they need to do and what they can expect. We appreciate the continuous monitoring performance management, making it clear that continuous monitoring is on the agency, and the agency partner is responsible for tracking and managing that CSP, we're if the midst of doing that right now with one CSP. We have been able to pull that document out and say over and over again, we need to have a conversation with the CSP and agree to the terms to do U.S. monitoring now rather than come back later when they're operating and they're going to say, you didn't tell me we need to provide these things. It's helpful to have the conversations early on and appreciate FedRAMP has given us those.

We also appreciate the FedRAMP and the collaborations that go on there and conversations. I know, Ralph is usually on a lot of these cause. I appreciate his questions and some of the ideas. Makes it easier to benchmark against what other people are doing, seeing if other issues are coming up in other agencies and how they're addressing it. We appreciate FedRAMP's push to get our agency liaison group together.

Some of the pain points we're experiencing, as a consuming agency or agency partner we fully understand it's our responsibility as an agency to identify, privacy Cloud Services that we are using. Our current information source for that right now is the FedRAMP portal. And we have found some serious errors and issues with the portal. We use that for our continuous monitoring efforts for tailoring, for implementation, looking at Comm test and liability management. It's a key tool for our security treatments to be using in our come minus teams. Unfortunately it is often out of date, missing necessary information for our security officer and compliance team to perform their work.

Examples of that continuous monitoring and problem reports are missing, one provider had it missing for over eight months. They weren't aware of the FedRAMP portal. We had difficult time identifying migration efforts from the CSP so we can migrate our control. We find the customer responsibility matrix and SSP do not align and match. Controls offered in one place are reported as customer responsibility in another place.

It makes us tricky to tailor it appropriately and under the risks. One of the ways we have tried to address this when we stood up our review teams in which a team, apart from our security officers go into the portal, review these things, mark down the deficiencies, reach out to a CSPs, and work to get those documents needed, work to get answers to some questions that are needed. We also do a supply chain risk management assessment at this point as well.

So that if there are other things that we need to know about and risks we need to take on, we can do that. It's been a valued security officers doing their job so they understand the risk that they need to address, mitigate, manage or even accept.

We also are seeing that the access process, the access forms are still very much in the handle process for us when we want to get access as a shopper or when we have issued an ATO to success a form and documentation. We are on our end trying to automate the form so that we can have a better flow of signatures and approvals so we can get that done faster to be able to get that to FedRAMP to get that information back. We'd love to be able to see online requests or access process that is a little bit easier to manage.

Also we are struggling with the lack of ability to assume the Cloud Service within our GRC tool. We understand that many Cloud Services do have an OSCAL progression in place. We look forward to leveraging that and try to get that into our GRC tool. I know FedRAMP is in the midst of acquiring its GRC. Another item, integration of other tools for disability for continuous monitoring. We have the CDM efforts in place. It would be wonderful if we allow the agencies to see the trends and risks in cloud utilizing some of these already existing tools, being able to ingest some of that material.

From there lastly we would love to see FedRAMP continue to act as a collaborative facilitator between CSPs and agencies. We're seeing few CSPs have collaborative groups. We find those helpful and valuable as a small agency when we're trying to ask questions or get information from the CSP. When we have to go to the CSP to ask about an incident or breach, many times it takes us a few tries to share that information with us so that we understand how to move forward.

I think if there were more agencies pulled together in that conversation, it would be more worth it to a cloud provider sit down with those conversations. We believe FedRAMP can be that connecting thread for that. And also can help with continuous monitoring, corrective actions, changes that might be impacting agencies. We feel that communication can happen more periodically. I think that's what I have. I'll turn it back to David.

>> Thanks, Susan.

>> David Meyer: I kind of sent a bit of an interesting spot. I started out at a 3 PAO. Then I got transitioned over to a CSP. And now I'm on the federal side.

So still waiting for opening on the FedRAMP board for the quad effect there. But definitely a lot of perspective.

I guess if the early days, one of the things I saw was a lot of kind of marketing and push from FedRAMP, from the FedRAMP team on getting it out there. I would say there were times when I was originally at that 3 PAO that they weren't sure was worth the investment to become a 3 PAO. I think I might tie it to similar kind of discussion from the previous panel where the 3 PAO also has to make significant investments in themselves in order to become a 3 PAO and remain a 3 PAO and make sure they get the CSP. Similar to the CSPs initial digging their heels in, the 3 PAOs also do.

I don't know if that's-- a tidbit to think about when thing about the lack of resources on 3 PAO side of things. But obviously jumping ahead quite a bit in the FedRAMP. FedRAMP outgrew itself. That's one of the things we feel here especially with the modernization and shifting the PMO and kind of reallocating the JAB offer of ICSPs. It seems FedRAMP was too successful for itself. And I guess some of the feelings we get out here in the Department of Education is, instead of kind of growing itself to be able to handle the volume, which I think a big part of this transition was the backlog of CSPs that we're not getting through the PMO reviews. It used to be four to six weeks.

And then it got to four to six months and obviously for CSP, that's very hard to work with. One thing which I didn't hear in the earlier panel which I want to mention, the agencies that I've worked on their cloud security team is, once a department has granted the ATO, that authorization allows utilization within that agency.

Maybe there are some agencies there that maybe aren't as mature in their process and want to wait to get that final approval from the office. That's another drag on those CSPs that are chomping at the bit, inviting them to the dangerous as someone mentioned earlier.

Maybe utilizing that a bit more from the agency side. Once you get through the agency ATO, you still need to go to get only the market place, et cetera. There is still that agency ATO, and you can carry multiple agency ATOs while waiting for that PMO review.

Some of the things that we appreciate and feel that works well with the FedRAMP process, definite standardization. There was discussion about nuances and guidance that goes here and there. For the most part it's a pretty well oiled in not here at the Department of Education. We have 30 CSPs, a quarter we have initial sponsor for and a couple in the pipeline. The process, readiness, everything that goes on, it's pretty well laid out. Obviously some speed bumps along the way. That's something that we appreciate how all the agencies and all the CSPs are kind of, the ones that are familiar with it. And that might be, you know, getting the word out as successful as FedRAMP's been with over 400. I heard in the call, someone felt the 400 products out in the marketplace are, I don't want to say insignificant, but not as many as potentially could be. I definitely hear that. Obviously thousands of products out there that want to get into the FedRAMP pipeline.

Working with the agencies, one thing we do here at the department is when any of our stakeholders is looking for a product, we'll complete with them. If there's an existing product in the marketplace, we're not going to encourage them to go out and look for another solution. So you know that guidance that we give here will obviously limit brand new CSPs on the marketplace if that solution already exists. At some point the market place is going to be saturated with CSPs offering similar products and services. Some of the pain points we've seen over the years, again if my roles as 3 PAO and CSPs. CSPs have multiple platforms. Sometimes it makes it easier. Sometimes it makes it harder. You have the Adobe, Cisco and different products. Sometimes again when they streamline it, it makes it easier. When separate, something on the CSP side, they think they can pig piggy bag on the same set. If it's the same product fine, if it's new, they have to go through it again. Another thing I see with the agencies is we don't always need all of the features that a product is offering. So we're sitting there, going through an assessment or doing an internal assessment for those initial CSPs. And they have all these different features creating issues with their assessment and trying to do all the stuff. We only need the features.

Sometimes the rub there between the agency and CSPs, I don't want to cut back on what they're offering because they have an agency they're working with. At the same time do we want to incur the risk of an entire full suite of products if we're only using two or three with that?

Another thing which I think Susan I mentioned with the liaisons, you know it is very helpful. Sometimes when we're working on the continuous monitoring or the multiple agencies, it does get interesting.

One agency's okay with the significant change. Another one wants to review, test, et cetera. Even there's guidance there how to do the multiagency monitoring, getting all the agencies onboard to go the same way I think would help with some of that rub there.

OSCAL was mentioned as well. Waiting upon CSP for those adaptors. The GRC tools out there that haven't been able to provide OSCAL capability. That's hard for our adoption. There's a CSP out there-- if we don't have the tools on the other side of the house to be able to ingest and process them, the OSCAL is not going to work as intended.

And another thing-- you don't want to hear from the other agencies or whoever is on, on the OMB mandates and CISA, we take those seriously of our FISMA system have to be complying with those. When we work with the CSPs, we haven't gotten any guidance with the PMO yet. So I would say the OMB mandates and CISA BODS, FedRAMP is a little coy sometimes in our impression of sending out those mandatory guidance to the CSPs. Puts the agencies in a little bit of a tight spot when our business systems have to be up to par in one of those, whether it be zero trust or whatever else. We go the CSPs and they're not participating at the level we need them to. That also introduces a certain amount of risk which we kind of need the PMO, the FedRAMP board to have our back and kind of reach out to the CSP on our behalf. If you're going to be a part of this FedRAMP process, you know, the CISA bods, they're serious stuff. And you have to step up. I guess that's the long and short of it from the Department of Education.

>> any of our committee members, do you have questions for this panel? Josh, go ahead.

>> Josh: Thanks. This is Josh from the department of veteran affairs. Something you questioned around, the effect of a certain number of similar products in the marketplace and how that affects the larger marketplace whether it's worth it for a vendor, whether you would even suggest a customer within your agency pursue a person new thing when there are several things on the market place where one thing that is already approved.

Two questions on that. One have you had any push back from anybody in your legal or acquisition side of the agency on the potential impact on that, things like competition and rules there concerned with. And secondly do you feel like that happens when there are multiple products available or is that happening when a product is available? So along the lines of it being a separate category, maybe we don't want a fifth one. Do you see where people get to one and people go there's one, and that's what we're going to have to use because we don't want to go through this again.

>> David Meyer: Appreciate that. I mean, I'll say that, using a sim tool, for example. Obviously we're not endorsing any products here. But let's say-- one of them might be in the department. And a new office is coming and saying, hey, we need a sim tool. Definitely if we issued the ATO already to one of those sim tools, we say, it has the department of ed ATO. Look at that. It's going to be their decision if they want to go that route.

And then in the event they came to us on a certain product, again let's say sim tool that they need, even if we have not issued an ATO for any sim tool, it's in our best interest to say, check the FedRAMP marketplace first because, when you think about it from our perspective, from the agency, engaging with a sim tool that is not FedRAMP authorized by any agency versus a sim tool that already has an ATO, the level of knowledge base and everything, you know, we don't need to start from scratch. Right?

So have the legal ramifications of that. But from our process of A, either engaging with the product that we've given the ATO versus and also kind of through the onboarding process, if one sim tool has an ATO in the marketplace and the other one doesn't, we're generally going to go with that. Again using sim tool as an example.

If you're a new player and you're on your own sim tool and you see the federal marketplace and see four sim tools out there. You think to yourself, even if we found an agency to sponsor them, just by virtue of being in the marketplace-- Federal Agencies looking around.

Again accounts I haven't thought about the legal respect identification. On the practical side, that's how we review things.

>> I understand you have a practical side of it. Along the lines that you don't have a contract in place. Just that the vendors-- (away from mic) within that marketplace, and personally we had difficulties with the law around that, on our side because it comes up a lot. Thank you. That was-- (audio breaking up)

>> Susan: Susan. Our board looks at anything new. We have our presume folks and legal sitting on that board. What we ask when they come in and we have that offering, the business needs to show how that offering does not meet the requirements, whatever thing they want to use instead does meet the requirements better or is a better product or is a different product that they'll be able to utilize else are with. They need to make that decision on do we need to put another thing into the TRM and approve that, or would it be better to go with what we currently have that's already initiated that's operating, that's already being monitored. And I know from the TRB it's a tough sell for these folks to say yes, we have this. But let's add another version of it or another flavor of it to this. The business has to then do the market research, show they tested the current tool and they tested out what they want for the new tool, they did the demos and understand the requirements. It helps our businesses hone their requirements and our legal team can say, they've done this work and documented that many now we can make a decision to move forward with the new item or stick with what we have.

>> Josh: One question on that-- when you don't have a contract in place for that legacy thing what you're saying is the preference. Do they support pushing back to that question, you must use-- that tool and then limiting competition on the contract. You would have to go to that tool. Is that something you've done in the past? You've seen the lawyer and the contracting support that as a reason?

>> We haven't received any of the push back you're talking about. As long as it's very clear and documented the TRB board stands.

>> We have a tool for that. (audio breaking up)

>> Do any of the committee members have additional questions for this panel? Thank you so much, Ralph, David, and Susan for joining us. We're going to the final topic. Larry would you like to kick us off, key takeaways and closing remarks you may have?

>> Larry Hale: Yes, absolutely, Michelle. I have my right tabs in line. First of all, thanks to all of our speakers, our guests, the presenters, guests, Pete, Ashley, Laura, Jim, Brian, and Tom, and also Ralph, Sue and David and for the committee members for the questions you asked.

This was really a phenomenal session for us in terms of the information that you shared, the insights that you shared. It was extremely helpful. For me, you know the biggest takeaways, and I do want to just prime the pump for the committee members. I hope you have all been taking notes and getting valuable information.

The first item, takeaways, that OMB did really listen to this committee's feedback in the preparation of the memo.

I appreciate the emphasis that OMB put on, automating the process with digital packages using OSCAL which is something this committee should look deeper into in terms of identifying and documenting our ways to expedite the authorization process which is one of our priorities.

Process opportunities within this digital authorization process to expedite authorization. From the industry panel, the need for additional FedRAMP staffing impacting the timelines and bottom line. I'm thrilled Pete is here listening, talking to us in the beginning and participating in this meeting. This is a challenge, you know, Bill has identified this in previous meetings, Bill hunt happen. In terms of FedRAMP's budget and recognizing it's limited. It's an opportunities for Bill, for Pete as the new Director coming in frequent from the outside to bring that fresh perspective.

The inconsistency of guidance, where is it inconsistent and how FedRAMP can improve and clarify and hopefully simplify its guidance. What are actionable solutions that we are in our committee to propose to reduce that inconsistency? And the lack of 3 PAO resources and experience is at the moderate high level which are causing bottlenecks and delays and increase cost. How can FedRAMP better support the 3 PAOs at the moderate higher level in what actionable solutions can we propose? What are ways FedRAMP can support expediting this process? And from the agency panel, again, inconsistency and reporting in between CSPs, reduced monitoring and where there are deficiencies how agencies struggle with how to escalate and resolve those in timely manner. What can FedRAMP do to standardize on this what actionable solutions can we propose?

Disability will support for CSPs that are new to FedRAMP additionally struggle to afford the FedRAMP authorization. What can we do to support them more and what actionable solutions we as a committee can we propose. The FedRAMP issues. CSP unaware-- information located in different places, being hard to find.

Again, actionable solutions that we can propose as a committee and important the accessive collaborative-- what actionable solutions can we propose in with that, that summarizes my immediate takeaways, first my initial notes.

Let me open it up to the committee members to invite your observations and your notes as well, please.

>> Hey, Larry, this is Mike from Google. I have a quick question. If we had questions for Pete that we would like him to be able to answer, is there a format or a way for us to submit those to Pete?

>> Larry: Pete's right here. Pete, are you about to go off mute?

>> I am willing to state that, the public is free to email info at FedRAMP.gov for any inquiries and questions, et cetera and tag me into those. And I will make sure that someone on my team responds to all those. I actually don't need to do that. You're doing it already.

>> Excellent. Thank you, Pete.

>> Mike, if you have questions that you would like discussed in (audio breaking up).

>> I'm sorry, Michelle, you're breaking up really bad. Maybe if you can put it in CHAT.

>> Larry: Yeah, we lost it-- it went garbled after that.

>> If you have questions, just email me.

>> Okay. Thank you.

>> And Matt, you're next.

>> Matt: I think I hit all the buttons here. Yeah, thanks, Larry, good summary. I mean Josh's question was my question. And you know, maybe this is more of a deeper thing to poke into. But the initiation and sponsorship business processes and the potential unintended consequences to the markets and accessibility to markets by agencies-- was an interesting thing that kind of popped up there; Josh, maybe you can help me. That was my question but you beat me to it in the end. And the other thing I have is, and I touched on this, this might be a deep every thing as well. The red teaming inclusion and the OMB memo, hear be dragons. There is a lot of nuance and important nuance and including this, and an assessment program around disclosure and data ownership. And vulnerability disclosure program adherence and equities for the government who owns what is discovered, all of these issues that go along with a red team really need to be exercised and kind of contingency plan before something goes into place. Those are my two-- that's what I learned today.

>> Larry: Great point of the the important of exercising it. Thank you.

>> Kayla: One of the things I felt I heard a few tiles was the need for real legal clarification on risk acceptance and responsibilities for that, for the agencies. So actually making it very clear the principle of adequacy is-- to be able to actually do that legally. So I think that stood out to me as something that was brought up a couple of times somebody needs to tackle. Maybe we can make recommendations there.

>> Josh?

>> Josh: They did a good job of restating my thought. [low volume]. Even when they have not sponsored something, not sponsoring has an effect on the market if that makes sense. And I would very much-- [low volume] the red teaming is something I hear a lot within the agency. And getting clarification-- [low volume]. Further clarification required.

>> All right, Bill?

>> Bill: I want to put one thing here. I thought that was fairly consistent throughout. And contributing factor for some of the delays, corresponding the process. You know, one relative to guidance and the inconsistency in that guidance. This will be 3 PAOs, advisors, agency sponsors, FedRAMP, as well as the leveraging agencies clearly, if everyone is effectively going through and hearing something different, you can see that as being a contributing factor if not a significant contributing factor in delays, rework, costs to vendors, 3 PAOs, and then the other aspect is rework.

Understanding what work is being done at the 3 PAO level of the advisory level by assessors, by agency sponsors, by the PMO. To me this is a classic case of program and project management. And essentially going through and looking at this in a singular work stream with the work effectively broken out as a project across those individual components of that work stream versus looking at this more broadly as separate work stream at different points in time with different stakeholders having individualized responsibilities. I think there's a clear eyed opportunity around looking at the entirety of the assembly line operation in a singular work stream that actually has key stage gates, particularly relative to the performance of work and the associated quality checks at that point to ensure that everyone is essentially operating with a common set of expectations, particularly relative to adequacy.

And what benefit that provides is then mitigating some of the correspondence around reassessment, rework, rereview of the package and its entirety or parts of the package and its entirety that contributes to some of the things that we've heard around. We achieved the FedRAMP agency authorization and waiting six to 12 months waiting to get into the FedRAMP market place. I think there's a clear opportunity to look at this as a work stream with multiple broken down parts that have to effectively have visibility and transparency working through and set of expectation.

>> Kayla: So to add a little bit, within guidance. I think it touches on the different things we talked about. Engaging in the discussion of how do we bring this forum that is publicly available maybe FedRAMP ecosystem available to help with clarifying processes to help with adding best practices to help with details on controls where the community can talk about these things. So even if it's separated between the different components. We need a place for that conversation to happen freely. Joshua and Bo you have your hands up. Do you have anything else to add?

>> I'm sorry. I do not. Apologies.

>> Anything else? Any final thoughts on that?

>> This is Bo. We need to do more of this. I think the challenges we see across the various key stakeholder groups in a way that reflects assessors, advisors, vendors, agencies, program as well, as well as the agency sponsors. I know we heard from two key constituency groups, one leveraging organizations another Cloud Service providers. It would be interesting to go through and take a look at this from vantage point of sponsoring organizations, leveraging organizations, 3 PAO as well as 3 PAO advisors. I think we need to hear more of this. And today's discussion, in my mind has been one of the most vibrant we've had in a long time. And I think some of this truth, and absolutely that, I've been in agreement with much of that which was stated today. It's important for us to properly diagnosis the challenges to properly solution them. Over.

>> All right. Thank you much so. Larry, do you have anything else for the meeting today?

>> Larry: Absolutely. Honestly with Bo's remarks there, Bo could drop the mic. Really, thank you all. We had a great turn out today. Lent presenters, excellent speakers. And as Bo said lots of truths were spoken here today. We have captured it. A great turn out on the committee, too. Really strong attendance on the part of the committee members.

So I really appreciate that. I'm glad we all heard it. Thrilled you are here and state through the whole meeting, Pete. For the committee, thank you for sharing your thoughts. Also the members of the public, appreciate your participation, your giving of your time to participate, to listen, to hear this.

And we do welcome and invite, understanding that we have to limit the time at the beginning of this meeting. We welcome and invite your comments through the public comment portal. And depend, thanks to all the committee members who helped get the word out because we did see a significant increase in public comments due to people getting the word out, putting it, inviting public comments through social media channels, et cetera. So definitely it helps. We need, in order for this committee to be effective, we need to hear those perspectives. And today in this meeting we heard a lot.

Now that we have this discovery phase done, in the next meeting, please take a look at your notes from today. Come prepared with these notes from your independent research as well as from the presentations and discussions today. And be ready to brainstorm actionable recommendations on these two priorities.

Lease again also take notes of the public comments. Our outreach has been successful with high increase of submissions, review the comments as they are helpful in helping us better understand the issues. I look forward to our next meeting where we'll work on developing structure for our report and recommendations in our two priority areas.

So again, thank you all for your diligent and thought. Work to improve the process for the secure adoption of cloud computing products and services in the Federal Government. Michelle, back to you.

>> Michelle: Thank you, Larry. And thank you all again for joining this meeting today. With that I will now adjourn this meeting at this time. Thank you again.