*7444257*

*Federal Secure Cloud Advisory Committee November 2024 Meeting*

*November 14, 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, we're going to give folks a couple of minutes to join, and then we'll go ahead and get started. Thank you.

And if you're joining us, we're going to give people a minute or two to join. There are some people in progress.

Good afternoon. Welcome to the November 14, 2024 meeting of the Federal Secure Cloud Advisory Committee or FSCAC. My name is Michelle White and I'm the Designated Federal Officer, DFO for this Advisory Committee. I'd like to thank all of our presenters, attendees and stakeholders for joining us today and those who have provided public comment.

Public comments submitted via the FSCAC public comment form by Wednesday November 6, have been provided to our committee members. Before we start, there are a few things that you should know. This meeting is being recorded via Zoom. This Advisory Committee is also statutorily required under the defense Authorization Act for fiscal year 2023 and established under the FACA as official filing date of February 28, 2023.

This committee is considered a Federal Advisory Committee requirements under FACA. My role is to manage the day-to-day administrative operations of the committee, attend all committee meetings and ensure that the committee operation in compliance with FACA. The duties of this committee providing-- agencies on technical, financial and programmatic and 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 FedRAMP Authorization Act of 2022 statutory requirements. And it proposes to specifically examine the operations of FedRAMP and determine ways the authorization process can be continuously improved. Collect information and feedback on the agency compliance with an implementation of FedRAMP requirements and to service a forum that facilitates communication and collaboration among the FedRAMP stakeholder community.

I will go ahead and go through a role call. Please let me know you are here by saying you are here. Larry Hale.

>> Here.

>> Michael-- here. [Roll Call]. Carlton Harris? Kayla--

>> Here.

>> Josh Krueger.

>> Here.

>> Daniel pane.

>> Here.

>> Marcy--

>> Here.

>> [Roll Call]. Bo.

>> Here.

>> [Roll Call].

>> Bill hunt.

>> Here.

>> Joshua Cohen? All right. Thank you all. It looks like we've a quorum established.

So the purpose of today's meeting is to continue drafting an initial set of recommendations for the committee's first two priorities. The intended outcome is clear, documented set of initial recommendations for the draft report. Again these are not final. And will not be voted on today. So the goal is to get the recommendations as close to a version of done as the committee feels comfortable with.

For our agenda, we are going to have our welcome to call order that will take place from 12:00 to 12:10 and jump straight into public comments until 12:30. Followed by Chair remark until 12:35.

Next we'll dive into our continued deliberations from last meeting. Discussing any additional individual discovery and capture initial recommendations live in a draft report until 1:35. We'll follow that by a shorten minute break until 1:00 what. Following the break we'll spend the rest of the meeting, continuing the committee's deliberations on the initial recommendations. And then we'll end the meeting no later than 3:00PM by sharing our next steps and closing remarks.

At any point, we end the agenda item early, we'll move forward in the schedule. Onto the next item. And allocate the initial time to drafting the recommendations.

Housekeeping items for committee members and speakers today, please be sure to identify yourself before speaking so those listening online or reading the minutes after the meeting will know who made which comment. This is a virtual meeting. Please make sure that your microphone is muted any time you're not speaking. When it's your time, when it's time for the committee to deliberate and you like to raise your hand. Click on reactions button on the menu bar and click raise your hand and click lower your hand if you're done speaking. If you send us a chat to the producer with the content you'd like to add to the report which is encouraged, please be prepared to raise your hand and discuss with the committee what you have send to the producer.

Only the host of this meet can see the CHAT responses. Others may not know who submitted what comment. Lastly, if you are not a committee member, please hold all your comments until the public comment period. And again please ensure your microphone is on mute otherwise.

All right. Let's go ahead and move to our public comment period for on our agenda today. At this time, I'd like to welcome members of the public to share their comments. To our speakers, note that there is a timer that will be displayed on the screen, indicating your time remaining. Each speaker is allocated four minutes to make their comments. We will be interrupting speakers who exceed four minutes of succinctly and be respectful of the time. As a reminder, all public comments submitted by Wednesday, November 6 were presented to the committee members prior to this meeting. Our producer will take us to our website, show us the location of the public comments that we've received so far.

It looks like we did receive one comment from Azim-- if you are available today, would you like to elaborate on your comment?

>> Sure. Uh, thanks for taking the time to hear this comment out. This comes on behalf of the CSP community. We're wrestling with the FedRAMP risk management deficiency triggers. They're designed to bring focus to Cloud service providers who are not performing adequate vulnerability management. And we definitely agree that it's a critical part of maintaining a good risk posture.

However, there is a challenge associated with that mechanism not delivering the right outcome which is essentially bringing focus to CSPs who are not doing their due diligence in vulnerability management. And it's primarily due to scale, not being taken into account and static risk triggers that are based on a finite number irrelevant of the denominator and size CSP. For example, CSPs. Each greater than 30 days, receive a DFR, the five plus rule applies whether CPS is managing a million host or just a hundred host. In a situation where CSP has five unique vulnerabilities greater in 30 days in a fleet of 100 hosts, five percent of the total fleet that's not patched they get a DFR. Another CSP may have five vulnerabilities but might be managing a fleet of one million host which is .005% of their fleet not patched within the performance guideline but getting the same level of escalation. At the time when FedRAMP resources are stretched, the CSP marketplace is expected to grow on a rapid place and-- are going to increase. We believe Fiscal Year recommended some enhance deficiency triggers to not remain static regardless of scale of the CSP. Deficiency trigger should be adaptive to urn vulnerability management at scale considerations. So really the question is, is the FSCAC ifs open to making a recommendation to address this challenge. If yes, how can they facilitate that recommendation?

>> Thank you so much. Moving on, it looks like we have another comment that came in today. Laura if you're available, elaborate on your comment.

>> So good afternoon, my name is Laura. I'm the executive Director the Cloud service provider's Advisory Board and member association representing CSPs across the federal cloud system. My question relates to reciprocity. The FedRAMP roadmap looks to increase the FedRAMP ecosystem in line with the OMB, strategic goal to rapidly increase the side of the FedRAMP marketplace. One of the primary contributors to this goal will be the outcome of the agile delivery pilot that hopes to remove FedRAMP approval for every change so long as the agencies demonstrates due diligence in the change management processes. Only federal civilian agencies will benefit from the challenge or reciprocity when a Cloud Servicing is approved high isn't addressed. The gap between FedRAMP moderate environments and those hosting the workloads will continue to be exacerbated as Cloud Service offering are approved in more rapid rate in FedRAMP moderate environments versus DoD environments. The CR process of FedRAMP have differently times, different processes and require approvals from various leaders within the organization. This challenge does not exist in the DoD workload since IL 4, though is automatically reciprocated. Would this committee be willing to make a recommendation to the GSA Administrator to influence the DoD to integrate L4, ill 5 into the FedRAMP process so process reciprocated. And benefit from the modernization benefits from FedRAMP? Thank you very much. (READING).

>> Thank you so much, Laura. Is there anyone else that would like to speak today to provide public comments to FSCAC? Please go ahead and raise your hand. David, please go ahead.

>> Hi. Good afternoon. My name is David. And I'm a principal at tandem Gov. And I'm grateful for the opportunity to speak with the committee today. I did not submit written comments but hope this will be clear. I currently work as a principal at tandem Gov. I work with a lot of companies that ask me one question. How long does it take to get FedRAMP authorization?

And as you can imagine my answer, it depends. I'm a former attorney, and so that question feels really natural to answer as it depends. But unfortunately for those companies, answering that question is really important because it is necessary for their decision-making processes about whether and how to invest in pursuing federal contracts and whether products should purchase see a FedRAMP authorization. Because answering that question requires a lot of guess work, one of the things I have experienced is the need to conduct better data analyses to answer the question about how long a FedRAMP authorization might take. Fortunately there is good data on marketplace or FedRAMP.gov I want to recommend them for publishing the information as a transparency initiative. I think that there is more to be done. Today I wanted to ask the committee to consider recommendations to GSA that would improve the transparency of that particular tool and one particular banner, specifically to provide more information about the queue. So in my experience, it's obviously impossible to know how long a specific authorization might take, but knowing where a particular product or CSP is in the queue and/or which stage of review that particular product or service might be in, can help improve the transparency and promote better investment decisions. And at the moment, the only way to do that is to go to marketplace.FedRAMP.gov or GitHub repository and make guesses. I recognize that data publication can be a burden, on the FedRAMP program, a little bit more transparency will go a long way to help companies and companies that help companies do a better job of shedding light on where they are in the queue, where and whether they should make investments in pursuing FedRAMP authorizations and help the public better understand the need for FedRAMP resources it needs to do it effectively. Thank you so much.

>> Thank you so much, Dave. Are there any other members of the public that would like to share their comments with FSCAC? Please raise your hand. Okay, looks like we don't have any other public comments today. So this will go ahead and conclude our public comment section for today. Thank you all so very much.

So we will now go ahead and transition to Larry, the committee chair for opening remarks. I will be able to answer FACA questions if they come up.

>> Thanks, Michelle. I want to say thanks to Laura, Azim and the public comments and also the comments we received in writing which also,, Laura and Azim did so.

So I want to start by providing a brief recap of our priorities and what we covered during your previous meetings. And then set the stage for our meeting today. So as a reminder, going back to our July meeting, we further refined our top priorities and decided to begin developing recommendations for the two listed on the slide.

And we were also given two additional priorities from the GSA Administrator. But agreed to address them after working through these two first. So our work today will continue to focus on these two priorities.

Now, during our last meeting, October 3, we agreed on our report structure. Keeping the same report structure from last year. And we began to draft the problem statements and recommendations for two initial priorities. So today we'll continue deliberating and documenting our initial recommendations in the draft report.

Further clarifying the problem statements and refining our thoughts down to a set of the initial recommendations for the two initial priorities in the draft report.

Please note today's overall-purpose is again to only draft and refine the report. Nothing on the report is final until we hold an official vote. The goal is to get to a close to a state of done that the committee feels comfortable with.

I encourage all of you to speak up with any key information or initial recommendations you'd like to propose. When you have a specific wording you'd like captured in the report, please either state it very clearly for our producer to capture live or preferably send it in the CHAT so she can copy and paste in the report. As a reminder, Michelle said earlier, if you send information to the host in the chat, make sure to raise your hand and speak to it so others know who added what comment to the report.

The response to the committee's request for updates on FedRAMP's roadmap, OMB memo implementation and last year's recommendations, we have decided to invite FedRAMP to present at our first meeting in the new year. This timing will allow for comprehensive updates as plans are in the properties of being developed and finalized. Additionally, we welcome any requests for speakers or panels the committee would like to hear from during our next meeting to support the work on the next two priorities.

So what questions does the committee have?

All right. Were no questions, as a quick update, I'll give you a quick update on the social media status. Our FSCAC staff are working on getting a LinkedIn set up. I recognize it's taking a while. Sometimes things like this move slowly. Let's jump into our next item for today.

So this draft report was sent to committee members last Wednesday, November 6 for your review. In our last meeting we agreed on the report structure. And we began our deliberations on these first two sets of recommendations.

To ensure we address both priorities today, I propose we spend our first hour of deliberations on the first priority. Then move onto the next priority for the second hour. And we'll make sure we have about ten minutes to circle back for any additional comments at the end. Remember, we're striving to get to a state of done that the committee feels comfortable with. And with that, let's dive in.

Let's quickly review the rob at the same time and recommendations and start from there.

>> This is Bill. Do you all want to dive in and tear this apart or are we stating here?

>> We're not staying on ceremony. We're giving people time to read, catch up and dive right in. Anyone on the committee with initial thoughts, edits or concerns either on the problem statement as written or the draft recommendations we came up with last time. Bill, you broke the ice. Go for it.

>> Marcy got first.

>> You're too nice. Thanks, ill about. Marcy-- so I think this stems off one of the public comments we heard. When we're looking at priority number one in terms of like the significant entry, our action, specific recommendation number one where it says, reduce the time to authorization. My concern here is that obviously this is a big problem to solve. But there are a lot of factors that are 100% out of the control of the CSPs that's going through the authorization process. And my question or maybe concern is, is it worth us recognizing that within our recommendation, saying, there are all of these actions recommending, that would direct the CSP for the actions that they're responsible for and things they can control. However when it comes time to thinking of, well, they've done the implementation and assessment. They've gotten to, you know, reports delivery. How long is that going to sit at the agency?

And just wait and then furthermore, once the agency is issued, how long is it going to sit at the PMO. Those are times that are impactful to the CSPs and just, again, like, what else can be pulled? I don't know if it's worth recognizing that in the statement.

We have addressed some of the other factors in our prior recommendations memo. I do want to state that. I don't know that we need to reach that but nodding to those other factors that are not addressed here.

>> Rehash.

>> Thanks, Marcy. Bill?

>> Okay, a couple of thoughts here. First, I'm going to come out and say, I hate number one. I just kind of hate it, you all. I have to be frank here. I think that we have already sort of a split out process already. You know, there are different stages that people enter into it. Moreover, as a federal employee, I just can't get behind the notion of someone saying that their FedRAMP authorized that aren't really FedRAMP authorized. That can't help me. I can go to the marketplace and look if see if they're in the queue for not. Good enough for now. This overlap laps strongly what we're doing here and talking about. 5A, I think where we're doing provisional ATO to allow it to happen. I think one is duplicative and unnecessary. And as a federal employee, I don't feel great about it even existing. That's one struggle for me here.

Sorry. I am jumping into priority 2. Already. I apologize. I'm way off the chart.

Ignore everything I just said. I'm jumping the gun. I'm on the wrong page.

>> Okay, Bill, we're going to do priority two in the second hour of today's meeting.

>> I was looking at the wrong page in my notes.

>> I appreciate your passion. We will scratch that and get ready to say it all again after the break.

>> Sorry.

>> No worries. Now back to priority one. And thanks, Bill. We needed that. Back to priority one, and Marcy's comments.

So any additional-- and again, if you have specific wording that you want to put in the CHAT to our producer, please feel free to do so. Wording changes but also please state them so that we know who they came from so that everybody knows who they came from. The producer is going to know. But for the record we want everyone to know. Everybody get their coffee today?

>> Thanks, Matt. I appreciate that. That I wasn't seeing. I have to change my screen here. Go ahead.

>> I'll let Bill or Michael go if they want. I don't mind. I'm not proud.

>> Let me do it quickly. Matt on my screen your hand is up first. And then Mike.

>> Okay, so I don't hate one. Hate's a strong word.

>> I'm sorry.

>> That's okay, Bill. I just didn't want-- anyway. What I guess I'm uncomfortable about one is I'm trying to do some traceability from the problem statement to the action.

So the problem statement says, barriers due to complex and costly compliance requirements. And then our action is reduce time to authorization. And so I'm-- what I want to do is link those two and how action one, actually will address the problem statement. And I think what we're saying in action one and some of the suggestions will potentially and even the short-term before completion or during transition or during phase in would increase complexity. And I don't know if it will or will not change cost.

So I think we just want to take a look at each of these in the context of if our problem statement is complex and cost while still keeping security is-- then our action is to reduce time.

I want to, you know, are we saying time equals cost or time equals complexity rather than what we want to do is reduce complexity and drive down cost through these actions. And then one of the potential side effects, it also reduces time. You know, one of the outcomes that could be solved. I'm just trying to wrap my head around linking those two together if anything I'm saying makes sense.

>> Makes sense. Yes it does, Matt. So yeah, I mean, as we drafted action one or recommendation one in the actions, we probably need to, as you did, try to trace those back to the wording in the problem statement to see if they, if we're not just implying something as oppose to clearly stating something.

So obviously changes in wording are, edits are welcome. Let me call on Michael. And then Bo.

>> Sure, this is Mike from Google. I have recommendation based off some of the feedback from the CSPs in the public comments metric we can add potentially to this priority. And Darcy's adding them in right now.

So just adding a new action for which would be, basically adding effective measurements for one, two, and three. And then I put through recommendations, they're top level right now. We can always add more, debate them or take them out if you think they're not correct or we need more metrics. But just trying to help us get more specific and move forward on this one.

>> Thanks, Mike. We see the changes appearing in front of us on number four. And appreciate that. As we digest them, we can certainly come back to you for those questions. Bo?

>> Larry, good afternoon, and good afternoon to all of our public stakeholders as well as committee members.

Just administratively here, 1B is an extension of 1A or should be rolled into the main recommendation because there's no action tied to it. It's just a qualitative statement. We're talking about what the effect would be of a corresponding set of recommendations associated with 1A presumably. I don't know that 1B itself is a recommendation.

So having said that, I think part of the related recommendation that we can roll into priority number one, I think we have a challenge particularly relative to expectation setting. And there in we can go through and do a better job of defining expectations particularly around communication, quality deliverables look like, transparency and adherence to schedule. And you know, as well as going through and providing related material around time to achieve authorization as he had talked about. It's a known unknown. We are essentially a black box of sorts. And vendors are making multimillion dollars commitments small and large, and sometimes they achieve a FedRAMP authorization and end up seeing no business coming out of it.

So just being able to go through and set those expectations what a FedRAMP authorization means, what the cost correspondent to those actually are, how much time can actually go into it and he's absolutely right. It depends.

And we can help to clarify that it depends answer by identifying a set of prerequisites relative to the meaningful management technical operational type controls that should be in play. I know FedRAMP has a program corresponding to the FedRAMP ready process involving a set of self-assessments. But I think some of those things often times get missed. They're in part of the communication make sure organizations understand, the investments they have to make, the level of documentation, the level of technology controls that have to be brought to bear. And so expectations management particularly relative to ensuring both initial commitment as well as ongoing commitment to the program are really fundamental.

So there is an opportunity for us to go through and set a recommendation that we send over to the GSA administrator that focuses on having the FedRAMP board or the FedRAMP PMO more clearly enumerate some of prerequisites to clarify some of the questions likely to be asked across every organization as they look at the the FedRAMP opportunity and whether this is right or wrong for them.

>> Thanks, Bill. Kayla, you're next.

>> Okay. Um, so I wanted to first off look at our step number one within priority one. And if we're really looking at the priority being identify public document, challenges to propose solutions around the barrier to entry-- I'm wonder if, one, in its entirety almost fits better for priority two. Since priority two is specifically around expedite authorization process.

In my mind, I think expedite is a timeline related. So as I was thinking through that, I was thinking is priority one, we're wanting to identify barriers to entry for the ecosystem? Right? Is barrier to entry, we're wanting to identify the challenges that keep people from it FedRAMP completely. That's like a good question to ask ourselves here.

barriers to entry from keeping people from participating in the FedRAMP ecosystem completely? Or is it more barrier to entry as it's clogging up the roads to become fully authorized? In that case, it almost really, one and two start to blend together. I don't know that I necessarily have a direct set of other recommendations based sovereignty that. It's a good question we should ask ourselves. Barrier to entry, what does that mean for this? And our recommendation should be tied back. These recommendations being tied back directly to actions achieving the priority. And then, yeah, I said, I would vote that one, fits better into achieving authorization than from people not being able to enter into the FedRAMP ecosystem.

>> Good point, Kayla. I think that supports the point Matt made about reducing the time being not necessarily addressing priority one. But your point it does directly address priority two.

And what does the committee think about barriers to entry? Is it as Kayla described, things that absolutely stand this the way of somebody getting into the FedRAMP process, deciding to use the FedRAMP process and that's absolutely a valid definition. And have we interpreted it that way in our recommendations? So what about thoughts on moving one down to priority two? And is there any objection to taking action recommendable specific recommendation number one and moving it out of priority one and into priority two? So we're not throwing it away. We're just moving it.

>> I think that makes sense, Larry.

>> Thanks, Bo.

>> Yeah, that traces better.

>> Yep. And thanks, Matt for bringing up the traceability and Kayla for pointing out that it's a fit under priority two. Which we're going to spend the second hour talking about. And now, Bill it's no longer number one that you mate. It's number two you hate. We just stuck a new number one in front much it.

All right; I do appreciate how the public comments that we listened to at the beginning of the meeting tie into these recommendations. And certainly the things that we recommend here can help address those issues. Kayla?

>> Just to continue along. I like now the new one here for priority one, thinking through this, I feel like creating this assistance program would reduce barrier to entry because helping organizations who don't have-- they're not in, they're not in the queue, haven't started yet, I feel like this is a good example that we can recommend that is going to encourage more organizations to try and get into the ecosystem and also help them do that.

So I kind of just helping to circle back to what we think barrier to entry means. I feel like this one whether or not all the details are perfect in it, does fit that mantra. Just want to throw it out there.

>> Thanks, Kayla. Appreciate that. And next hand up is Marcy.

>> Thanks. Marcy. For this, the barrier to entry that we're trying to solve is that there are unknown or misunderstood security requirements, CSPs may not know where to start or need additional clarity for numerous technical requirements they're facing.

I would caution about the realistic nature of this. I think it's a great suggestion. But I don't know that consultation provided by the PMO is realistic here. I think if we can lean on maybe turning this a little bit to focus on more clarity and what the requirements are and what the guidance is on that versus more like consulting in nature. I think that might be more successful and/or realistic in the current program structure.

>> And more scalable.

>> Correct. Correct.

>> That comes back to Bo's suggestion about more clarity. Clearly identifying instead of prerequisites. And Bo, you have your hand up next.

>> Yeah, just coming back to one again. You know, moving one down, the original one down into priority two, looking at what we have residual under priority one. When we're talking about an assistance program we have to go back and ask and answer the questions including the ones raised earlier, particularly around what does FedRAMP mean to me?

What opportunity will it effectively provide? We need to answer that question. Yes, it's a federal requirement. Agencies have to use CSP conclusions that are FedRAMP authorized. You got that. Next step, what are the requirements? You understand the requirements, you baseline against your architecture in terms of determining the lift. Being able to enumerate across impact versus an opportunity statement in terms of whether the investment is going to effectively bear itself out for a commercial organization that has a for profit motive.

Once we have gone through and answered, that how do we find a sponsored organization? Like I would love for us to go through in the set of actions that are identified or the recommendations identified, ask and answer some of these basic questions including setting those expectations around time, cost, how effectively baseline around initial hard to implement capabilities, technology related especially. And then what do I do to get a sponsor? Like how that process should effectively work. I think the requirement is on the government, on the PMO to be able to go through in clearly and transparency answer that question. We heard through the committee meetings over and over again the challenges that organizations have in terms of just wanting to find somebody that they can collaborate with, understanding that they've already made the strategic decision to take part in the FedRAMP program. I would love for us to be prescriptive. Right now it's high level. These recommendations as written can mean anything in my view.

The more prescriptive we are, the more and better effective we are as a committee.

>> Great. Great. More prescriptive in our recommendations and prescriptive in the outcomes that we expect either the FedRAMP PMO or the board to respond.

>> This is Marcy. If I can build on something Bo mentioned. I think the part about the government providing PMO providing clarity and maybe facilitation is too strong of a word. But regarding agency sponsorship, it's the only way to get into a FedRAMP authorized status at this point. And unless there's an update the FedRAMP program can share around the program authorization path, that is it. And so, and we've heard to everyone's point, agencies are increasingly unwilling to sponsor for a variety of reasons. That is a significant barrier to entry that we are not addressing. I think it's worth expansion on that. And I can work on words and put something in the CHAT.

>> Thanks, Marcy. Awesome. Yeah, I mean, honestly, in plain language, identifying the real barriers and formulating our recommendations to address the barriers. And it may just be a more clear prescriptive how to with actionable checklist of steps to go through.

And you know, more than that, resources to tap into, to help you figure out the next step.

>> And Larry, if I may, I would identify the sponsorship challenge as a explicit recommendation as oppose to going through and capturing that. It should be a 1C.

>> The sponsorship challenge is a barrier. That's essentially what we're saying.

>> Correct.

>> So let's do that.

>> I think it should be outside the technical assistance program. I think it does need to stand alone but probably as two or three, not 1C.

>> Yes. Totally agree with Marcy. And I think the work product here can literally be a rubric and a guide that helps organizations understand not only the requirements and the why they have to do FedRAMP. But the how to get started. And I know FedRAMP has a get started guide. And this might be a corresponding update to that or a stand alone document that helps to go through, navigate the key milestones, the key decision markers around being able to go through and achieve. Short answer right now is they reach out to the PMO and sometimes it's a bring me a rock. They reach out to our organizations that are providing advisory and counsel basis and they only know what they know. Not to say there's a challenge gap there, but they're probably reaching back out to the PMO. And it's just best for the PMO to affirmatively state exactly what the pathways are and how to effectively navigate those. You

>> Thanks, Bo. Mike?

>> Hey, this is Mike from Google. I think we have multiple prongs on this particular challenge. And so like I'm looking at it from the perspective, I think we should definitely instructed GSA Administrator or advise, I should say, to-- we establish criteria that helps Federal Agencies determine the most appropriate for them to engage with. We should most likely simplify the process and standardization and consistency of the process from the FedRAMP PMO. And we should also potentially build and streamline the on-boarding process for the CSP along agency needs. I feel like there are multiple pieces of. It's going to be agencies, CSPs and FedRAMP PMOs. There's four distinct role in this that are going to be impacted. And I think we should clearly call out all four of those roles, the processes that need to be standardized for selection. And probably hopefully guidance on implementation timeline. This is the most impactful thing that is preventing the queues from being burned down today as reported by the CSPs. They don't have an agency, don't know how to select an agency and engage with the agency and not getting support from the FedRAMP program.

>> Bill?

>> I'm going to do the usual thing where I say something that might be wildly unpopular. I want to poke at this a bit here. As we're talking through all of this, it kind of brings to mind, I have run small businesses. I support small businesses, I want them to thrive. Not all small businesses with cloud product are suitable or useful to the Federal Government.

And it's also, this is still a very expensive and time consuming and laborious process to get through this stuff. I'm wondering if having more clarity upfront about the process and requirements and what goes into all of this for a business to really quickly understand like is this within something that I want to do or not. So they don't have to go through the process, we heard from the commenters in the past, years of going through the stuff and realizing there might not be a market for the product when we dumb out of the other side. I feel there are basic guidance that can be given. That says, look at the marketplace, if you see something that looks like your product, you might not want to go through this. This might be an expensive process for something the government doesn't need your service versus the ones that already exists.

That's not really the thing people want to hear, but there's two sides to it by being a small business, doesn't mean you better fold, you have the right to work with the government. That's why this process exists. Once you come out the other side, doesn't mean you'll have a custodies. I'm saying it out of love because I don't want to see anybody go through this and find it's not worthwhile. That's a fundamental fail for the Federal Government if people are going through all of these and spending money and not getting sales.

Everybody else is poking at it. Part of the guidance is talking about what this means in tangible terms, what the timeline looks like and cost associated looks like and be transparent, and some of these criteria I don't think we're being frank and upfront about today.

>> Yeah. The agency sponsorship being the agency wants to use you once you get through this or not.

>>Or will any other agency? Right. hopefully the sponsor-- otherwise you've got real problems on both sides of the fence. Beyond that, yeah, 100%.

>> Bo?

>> Yeah, let me give a little bit of voice to what Bill says like, some of our peer agencies here. We facilitated FedRAMP authorizations for dozens of vendors and today are actively sponsoring 19 service providers.

And for those Cloud Service providers we're sponsoring, it is a win-win type relationship where there's the fundamental need to go through and actively support the agency mission. And we have an able vendor partner that is active and committed to the FedRAMP. It's a true partnership and collaborative partnership.

I want to just highlight maybe a third area here. And this is a challenge that we're experiencing for ourselves from a Federal Agency perspective. You know, we recently had OMB issue the new FedRAMP policy memo, M2415. And within M2415 it calls out in section three the scope of FedRAMP specifically that it is applicable to cloud computing processes that create, or maintain federal information. Within that scope it calls out a set of exceptions. Exceptions are being misunderstood or improperly applied. And recent example I have is a federal, a technology service provider presently providing on-prem services is modernizing and moving outwards into cloud and providing their service as a service basis, as a Cloud Service provider solution.

And they spent a year building this out. And incorrectly presumed that one of those exceptions applied to them and did not have to achieve a FedRAMP authorization. After a year of doing this, they came back and, you know, after being told that they did have to achieve a FedRAMP authorization in order for us to use, they were literally months behind. So I this I some very specific guidance around the exception clauses enumerated in section 3, scope of FedRAMP, corresponding and 2415, they think this is perhaps not a barrier to entry but part of the actual applicability scope and understanding of FedRAMP overall that would help organizations a whole lot more clearly.

>> agreed. Thank you. Daniel?

>> Daniel from data bricks. I guess, you know, looking at that bullet two, part A, you know there are only a handful agency sponsoring the CSPs in the market place. I guess, maybe elephant in the room is how can we encourage more agencies to sponsor? Do we need incentive? Is there training? What would it take agencies to take responsibility and sponsor more CSPs?

>> Bill?

>> Bill-- money that would be the answer to your question. Appropriations are tight. Appropriations are increasingly tight. We still are under CR right now. Nobody's spending money on anything. Who notes what the budget foretells in the future. Again I brought this up when OMB first proposed it eight months ago. Money is not magically appearing for us to go through the authorization process. We are barely scraping dollars for ATO. Small agencies, there's no chance. As I mentioned in the previous, we are the ones who need the cutting edge tools because we are smaller and we need to move onto keep up. We need the special purpose tools.

So that remains a major barrier that quite frankly is entirely in the hands of OMB and Congress. I don't think that there's any nicer way of putting that. It is fundamentally a lack of resourcing that makes us unable to sponsor these things. And again we should be documenting that and upfront about it when finding agencies to sponsor this. There are few agencies that have the dollars these days to do this.

>> thanks, Bill. Kayla?

>> So hopefully I'm actually now very much looking forward to the new year update from the FedRAMP PMO around specifically the PMO being an entity that is able to sponsor/authorize new services, new CSPs into the marketplace. Because if sponsorship from an agency comes to a hard wall, it's not going to be feasible, there is no other solution unless PMO is, and I'm probably overexaggerating that-- there's no other solution except for the PMO being back up. I'm excited how that's going. How is the adoption of the PMO being able to response or these?

I might be using the wrote not terms here. This is going to be good for the group to chime in on. Because if there's no other way to help that for the agencies, then the PMO is the only other way to get these organizations in the FedRAMP marketplace in order for agencies to be able to use the newest, most awesome technology.

The one thing I would hate to see is a small company that has the coolest thing out there, looking at the FedRAMP marketplace, seeing an encounter come bent in there and saying, oh, nevermind. I'm not going to go for this because the incumbent is there. FedRAMP is expensive. It is true, it's not guaranteed additional business on the other side of that. So sorry, government, you don't get to use my awesome thing I've made. And I would hate for that to happen for sure on top of all the other, we want FedRAMP to be successful in order to provide secure solutions for the government to be able to benefit. Sorry. Maybe that was a ramble.

Sorry, wrapping up, can't wait for the PMO update on that.

>> Appreciate that, Kayla. I know folks from the PMO are taking notes on what we discuss here today. And I'm seeing hands and Bill, Matt, and then Bo. So Bill first.

>> Thanks. Maybe we can likes brief on Kayla was dropping for a second and bounce back and forth a little bit. Again I'm kind of torn across this notion.

For speaking for the federal ghost and Federal Agency, a small agency, I want to see the FedRAMP PMO if they're doing authorizations, focusing on the what the entire government can use. Focus on large scale, big solutions. A lot of times that's major providers we're talking about here. The value of the PMO is being able to authorize things that everybody needs, not little onsie twosie things that happen to be useful for one agency. The small agencies need to be able to do that instead.

I know that's not like, a popular answer, even more demoralizing for small businesses. But that's the value of it is do things that need to be done for the purpose of GSA. It's the General Service Administration. They provide general services that everybody needs for all government. It's centralized for that reason. It's the opposite of what Kayla's talking about that makes more of a barrier entry for small ones. There is the exception clause, the clause in the OMB memo that says they can prioritize specific services and tools needed that are up the queue as directed. AI is the thing that's now prioritized. AI has to go first because AI is the big thing everybody's doing this week.

AI is the important thing. If you have an AI tool, put it in there. Have I said AI enough? Have I met my quota? I think that's going to be a major piece of this. I think again, what Kayla says, if there is already an incumbent solution, it's going to be a lot of money for you to take your competing solution through the process. Is that money well spent, when we have the solution that does the thing? Again it's not popular but that is a stuff

A lot of times the answer is know. Federal Agencies pick one solution, that's the one they invest in and they use. It happens over and over and shuts out the smaller businesses. That's fundamentally how the government is designed.

So again I know that's not the popular thing to say. I love small businesses. That's kind of what we do. Happy for people to riff on that by the way.

>> So the order that hands are up is Matt and then Bo and then Marcy.

>> All right. I'm going to do a combo riff of the last three comments, I think. I'm not sure. I'm still processing Bill here. So I'm having a buffer--

So we keep saying that FedRAMP authorizations are expensive. But also FedRAMP authorizations are expensive. So if and when PMO authorizations other than sponsoring authorizations are going to be allowed or conducted, I think we have to have a global statement saying, in order to achieve these outcomes, there needs to be a significant and serious resource investment into the FedRAMP program in order for them to achieve the outcomes of both the recommendation and of the OMB memorandum with-- with the belief that this upfront investment will more than have a positive ROI by addressing the barriers and increasing the capabilities available to the government.

So that was a lot of words to say. Hey, if he with want to do this, FedRAMP needs resources in the time of credit and budget-- which may not come until February in the earliest to say this is a good investment as well.

>> Thanks, Matt. Bo?

>> Saddens me to hear Bill's comment. It is somewhat true. But it is reality unfortunately. But it saddens me largely because we don't want to be anticompetitive. And we don't want to effectively limit competition. We want to create a competitive marketplace where agencies have the ability to effectively go through and seek out through solutions not of my are all going to be exactly the same. That needs to be a foundational aspect of, the FedRAMP program and one of our priorities as we look at our recommendations.

Ed second aspect, it comes down to resources. There's an element of risk. You know, agencies don't go off and do FedRAMP authorizations because of a resources, and two, the corresponding cybersecurity risks and the impact of a breach that might effectively spill back over to them in terms of, well, the quality of the package, the corresponding risks that we have kept the alternative that may deem acceptable. Continuous monitoring to make sure the level of security achieved. So from the reverse aspect it's its own separate challenges. In terms of resources, how do we solve this beyond Congress and OMB?

One thing might be for us to go through and ask for specific recommendation to think outside the box, we have other models across government where vendors essentially go through and contribute into an initial into their actual standardization. If you're going through a miss-- to get your object module. Vendors go through and provide a fee to make that possible. So why can't we think outside the box around a recommendation, I'm not a lawyer. But realistically being able to go through and address the underlying root cause around resourcing because I can tell you that, if vendors achieve authorizations faster, it will end up saving them money.

And whether create more dynamic market opportunity we're looking for, making sure agencies have a competitive marketplace.

>> Bo, let me respond because you are correct in the NIST crypto module validation program. NIST has specific legislative authority to collect fees that offset cost from our validation laboratories. And this is part of our authorities to sell, create and sell standard reference material as well. FDA also does this as part of their process for medical device reviews where they not only collect fees, but for the FDA you can pay a fee to expedite your process for that compliance activity as well. There are other models that other agencies use to assist with costs.

It all comes down to what the authorities in the agency are in the end.

>> We write the laws through Congress. And we do policy. I'm sure if there is consensus and this is something that industry is wanting and willing to support there might be-- that's not the standard option but an additional option to be able to go through and address this fundamental need that seems to be constant. I can't even find a vendor to play with negotiable to do the work.

>> One of dark -- Bo to your point, one of the original ideas when FedRAMP was being conceived was charging an upfront fee to enter the process that would-- obviously the federal acquisition services mandate the cost. And that's a way of charging an upfront free to enter that process. And that fee would be levied, would cover the cost of the government services provided in the FedRAMP process.

So that's-- we can make a recommendation to that effect.

>> Yeah, just a cost for-- to go through and make sure, no one is looking for a sponsor. The resources are there whether it's through the PMO and capitalizes for the PMO to go through and scale operations. And I'll be honest, we should not be placing all our eggs in the PMO was set because they, too, are resource constrained. It's another avenue but one more avenue together with the existing sets of agencies. It's not going to effectively address the constraint that we have.

>> Thank you. So Marcy and then Jacque.

>> Thank you. I want to go back to Bill's comment, government-wide putting restrictions in place with the program authorization that PMO will be doing and that CSO authorize through that manner would mean government-wide demand, et cetera. We evolved to shall -- I we're not walking in circles because that was a key component of being eligible for JAB and being prioritized through JAB connect, FedRAMP connect.

Another piece of that, we're circling back to how is the CSP, going back to government demand of an offering, and the same way that they would try to attempt to find an agency response or. Providers don't always know what the demand might be or who their potential customer is within the government. It's a complete black box. And I think that problem still persists even in this idea if we start putting restrictions on that program authorization and eligibility to go through that.

So one, I want to be careful that we're not getting back into the same situation that we have been in prior to the modernization of other program. Separately authorization on the barrier to entry, there are impacts to other government programs. So if we start thinking about CMC and start thinking about every single Cloud service provider handling CUI in the DoD supply chain is going to have FedRAMP authorization or equivalency. It's kind of a side, you know, I think we would be remiss to not factor that in especially as we may see CMC being-- rolled out or required in other areas beyond DoD.

Lastly here in terms of-- FedRAMP is considered the gold standard. We see this come up when they're doing assessment, IRS 1075 assessments, CSP having a FedRAMP authorization having a higher-- it affects other programs. So I think we've got to find a way to increase the capacity of the program. And also the authorization paths to get there. They have to happen together.

>> Thanks, Marcy. Jacque and then Kayla.

>> thanks. I was going to address a couple of different things but to tag onto Marcy's increasing the capacity. I'd offer two thoughts which is there is a program called StateRAMP that we know about. And could we reuse the artifacts from StateRAMP inside of FedRAMP? How closely do they align? I don't know. And then the Department of Defense is working towards implementation of what they call a FedRAMP moderate equivalency memo to align with our acquisition regulations. And what this allows is a defense industrial based contractor who processes cover defense information can actually work with a Cloud provider using three PAO, the same FedRAMP artifacts to assert that they are FedRAMP equivalent. It will not go on the marketplace. We don't want to get people excited. It doesn't go on the marketplace but allows capacity again and availability of Cloud providers that are not on the market place to be used by our federal contractors. But at least put some rigor around those Cloud service offerings that these contracts are using.

I offer that to say that again, the use of artifacts potentially to move these from being allowed by, to be used by a Div contractor into how do we transition and use the artifacts to move them to a place where they actually are authorized for FedRAMP?

So I think we have capacity that's there that can be leveraged. It's a matter of getting to creativity about how we can reuse artifacts. I don't talk about reciprocity specifically. Using the artifacts, making sure it's okay. And what's missing? Again this is capacity, StateRAMP they are everywhere. Right? And the Div contractors, huge organizations, broad reaching. And so again, how do we start to collect this information to figure out what could be reused? And then my last comment is really just on the, really the documentation and the processes and procedures.

And I don't know the answer to this question. Hopefully we can get this. I don't know how much of FedRAMP's documentation and processes are actually worked with the cloud providers or commented on by the Cloud providers, getting soliciting feedback what is the burden of this? Does this make sense? How does this impact your Cloud provider? What is your comment on these processes? Is there a different way to do things that would be easier for the cloud providers? Clearly in the government we don't necessarily have the same perspective as a cloud provider or as industry does. So a tighter partnership even if it's a cloud security provider Advisory Committee board, using them as a partner to help us understand where our policies and procedures are not easy to understand. They're difficult to comply with. They're missing a specificity which is a big one.

But this would really improve the transparency between FedRAMP and our could Cloud providers and potentially get after some of these perceived difficulties that are there. I should say perceived-- they are difficulties that the Cloud providers have in understanding and implementing the guidance.

That's it. Thank you.

>> Thanks, Jacque. I think Marcy, is your hand still up? I think Kayla's next.

>> I still have more, but we can circle back to me after Kayla and Bo.

>> Okay, thank you.

>> Okay, Kayla here. So I did also want to throw in just another kind of anecdote about the definitely encouraging increasing capacity because one of the other things that's-- it's a positive really the artifact of FedRAMP is, that it's up-leveling everybody's security, not just organizations going into serve the Federal Government. The truth is, if you are a commercial entity working with a FedRAMP authorized commercial entity they want you to be FedRAMP authorized as well.

And so while I, that has both positive and negative side effects because it drives cost up for everyone because we're talking about how this is an expensive process, but it also increases the security cross the board which is a great goal. Something to keep in mind, not obviously-- we are focusing on the actual FedRAMP authorization process for the government to use these tools. But the byproduct of that is that commercial to commercial there's also a drive for the general vendor ecosystem to also be FedRAMP authorized. It's raising the tides all the way around. But it makes it even more critical that we increase capacity and that we do allow and enable more organizations to be able to achieve FedRAMP authorization anecdote. Sorry.

>> The theme of increasing the capacity is definitely one that we need to capture and build into our recommendations. So absolutely. Bo then Marcy.

>> Thank you, Larry. From the CSP Advisory Board during the commentary period-- [inaudible]. And you know, Jacque talked about StateRAMP which is awesome. I think it would behoove us to expand recommendation to capture the reciprocity opportunity between DoD DOI-- for FedRAMP high. That is valid recommendation. And I absolutely support it. And two, certainly going through and looking at the opportunities including StateRAMP. And then, you know, when you look at the context for M2415, that policy memo did go through and open the opportunities for other paths to authorization.

And it talked about alternative pathways that provide for the level of security that we need to commensurate with risk. StateRAMP absolutely whether it's ray low or moderate. And then industry broadly speaking comports with the type II security audit standard which is really focused on assessing a company's security controls initially and over a period of time. It's not commensurate with moderate but low impact. It might behoove us to take recommendation and expand that broadly focusing around the IL4 IL5 talk about StateRAMP and talk about market opportunities around security for low. And that would essentially go through and lease some of the pressure corresponding to usage of some of these existing authorizations to support root recommendation that we talked about previously the notion of step up authorizations. Can we step up low on a risk basis, maybe with a SOC-- an authorization that we can graduate to a FedRAMP moderate.

>> Thanks, Bo. Marcy and then Kayla.

>> Marcy. Thank you. Digging into the ideas of StateRAMP and reciprocity. What I consider in recommendations in StateRAMP is the PMO establishing a reciprocatory workflow. StateRAMP does accept FedRAMP packages. There no additional work needed. That doesn't work in the reverse. Currently FedRAMP does not accept StateRAMP packages, there were few nuances but the requirements are extremely limited in terms of standards and limitations between the programs.

If we're looking at things guardrails, timeliness, when the testing and timeliness of evidence was performed for that StateRAMP authorization, you know if it was performed by a StateRAMP or FedRAMP 3 PAO. I think there's a real opportunity to capitalize on that if guardrails are in place.

And then regarding IL4 and 25, our experience has been, you know. 5. There's some who reciprocity given from IL4 and 5, additional assessment is not required. What is required is PMO review. A CSP would go through I. Will 4 process, achieve that and then they have to go through the PMO review. They're are reviewing the assessment. From the PMP's perspective is they're going to view the authorization as any other agency authorization just as they would from HHS or any other one within the FedRAMP program. I think that's the barrier that would have to be solved is, respectfully why BI SA would get special treatment compared to any other organization granted. Lastly, Jacque on the FedRAMP equivalency, that's a valuable point. My only feedback on that is that CSPs are not going to pursue as long as there's a 100% compliance standard which is where it is right now. There are maybe zero percent, 1% of FedRAMP CSO that have 100% compliant. They're going to view, we need to get our actual FedRAMP authorization haves trying to demonstrate equivalency because they're different expectations and standards.

>> Thanks, Marcy. before I call on Kayla and Jacque, I want to mention that we have about eight minutes left on this topic. And if you have specific language, specific words that you want to get entered into the recommendations document, please do send them to the producers in CHAT. And we can, I mean, it's been a fantastic discussion. So let's move onto Kayla.

>> Yes, Kayla here. I wanted to call out that, we do have priority three on here which we're not two yet. But it discusses reciprocity. Although we have called put out. I know this is a priority given to us. Reciprocity, when we're getting to the point of priority three we might broaden that into general reciprocity. Because there is a lot of fantastic recommendations and topics discussed here that I think could fit into this whole priority and broaden this priority. Just wanted to call that out.

>> Kayla, thank you for calling that out. Appreciate that. Jacque?

>> Okay, I just want to address the reciprocity. Issue. In four, DoD has complete reciprocity with FedRAMP high. FedRAMP high reciprocates. FedRAMP moderate if you take the body of evidence IL4, we reuse a substantial amount of work that has been done. We do have general readiness requirements of connecting to-- similar to the tip. There are things using-- for often occasion. We have ten, just general readiness that the Cloud provider has to do. We have full reciprocity. What we do. And this is when you talk StateRAMP and FedRAMP, this is a good model is that when we go in in for an authorization, if it is a Cloud provider that knows they want to do DoD business they make sure the parameters are tested additional controls are tested. We worked really hard to make sure that we educate the cloud providers. And I think this is a key to say, when you go in to be authorized, say we're going to test the full body. So we pay the 3 PAO once and make sure the requirements are there. Retest once, reuse multiple so we can do the full authorization.

I think that's a good model that can be looked at. And I would say in five, we actually have, and I'm proud of this, less requirements than FedRAMP. So I don't know where we're going to sit on getting everything tested and who is going to validate the extra controls but we have less requirements. And so it's all published. But we do reuse and I would encourage to reuse that. There's very, very little difference in the requirements. It's really how we implement the cloud provider so that it operates within our boundary. That's it. Over.

>> And Jacque, I will call on Bo. Bo, earlier talked about us being much more clear and upfront about the prerequisites and the expectations. Do you have a model that does that? That establishes that so that CSPs understand clearly when they enter the process?

>> We do. And we use the exact same processes as FedRAMP. So we have, we use the LAR. Kick off meeting, architecture review. We go over the requirements. One of the big things we found with cloud provider we make sure that we understand what the SAP looks like and approve the SAP before going into the 3 PAO testing. We don't want to go through the 3 PAO testing and come back to us and say we missed something. Marcy mentioned which don't want DoD to get a fast pass. One of the big things that came out of our first year of recommendations with GSA was to allow any of the agencies to have their processes reviewed so that, if we met FedRAMP standards, that the authorization they would do what they call a low touch and do a spot check. It's not the complete review.

So DoD has done that. We piloted that program in the past year so that DoD, because right now we have almost 100 Cloud Service offerings under DoD PA. So that's almost a third of the marketplace. And so we do have a, we did get through that low touch process with FedRAMP. Because we reuse all of the same processes, procedures, that FedRAMP does, you know, really probably the only difference is the difference across everybody that validates the control, what does compliance mean? We don't have the same interpretation of control. You're gun going to have anybody, pick any five. You'll probably have one and a half agree that the other is correct. So anyway, it is not a pass. And it's not complete reciprocity but it is a low touch review so it can expedite. I would encourage other agencies through that. I don't know if they formalized the process from our pilot. But we both find the pilot helpful and useful the in evaluating processes and procedures.

>> That's correct, Jacque. We should followed up on that to find out if that has been formalized what the outcome of the pilot was. Bo? You have about the last two minutes, I think, of this particular set of discussions.

>> You know, Jacque just rang true all her entire comment.

But two thoughts here, each of the, the organizations and the sponsorships they actually have much of what we're talking about. Sounds like DoD does, GSA does as well. And it would behoove us to pull that material and collectively share out such that the engagement, the kick offs, the prerequisites, schedules, briefings, the corresponding prerequisites we look to are communicated outwards in an open and transparent manner. One thought.

The second thought, I love Jacque's-- controls comment. Largely because the set of controls corresponding for the FedRAMP baseline, Dave essentially stayed largely intact and grown incrementally over time. And you know, the the foundational question as to controls has to effectively start from why does the control exist and how does it specifically address inherent risk specific to Cloud? And a deployment model and delivery mod 8ling is diss terrific from a solution that is hosted in a non-cloud environment. All that to say is a recommendation to go through and review the FedRAMP baseline to make sure we focus on things that matter versus things that are nice to have but are not necessarily conducive to addressing an inherent risk specific to Cloud. That has always been an opportunity and we can programs see that as a recommendation and make that as an action.

>> That's correct, Bo. That was a great way to close out the first hour of our first discussion, our latest discussion on priority one. And I really appreciate-- what a great discussion. I know that it's been busy capturing what was shared. We are going to take a break for ten minutes. I can't wait to get back in and start talking about priority number two. And I think we'll let Bill go first. But thanks, everybody. Let's take a break. Come back at 1:45.

>> (BREAK)

>> Recording stopped

>> recording in progress.

>> Let's continue to the deliberations. Larry, overview.

>> Thanks, Michelle. All right.

So looking at our second priority. Let's take a quick look of what we've written as a problem statement as we did in the first hour. And I'm guessing that Bill will be ready to kick us off on discussing our concerns and recommendations for the second priority. So with that, Bill, I'm going to move to you.

>> Bill, SCC, let me start with the one first. Number four, here states, task OMB or FedRAMP or FedRAMP PMO, administrator does not tell me what to do. We make sure this language is updated what to do. OMB tells everyone else what to do.

So that's page four.

>> It's number five. You inserted the number one so everything slid down.

>> I'm going based on my document. Sorry. Number five now, everything is one plus. So that's my comment. Absolutely should not in the document, you're going to task OMB to do anything unless you're the President.

Moving onto the meaty pieces. Bo leads him very well to my overall concerns over a few of these with, let me-- number two which is I despise. Number 6A and then number 7 and specifically around 7C. I think all of these pieces of this, I'm really queazy about especially what the last thing Bo was saying.

For me, I think for the government as-- on the larger scale, the purpose of FedRAMP is not to just assess the controls that are specific to Cloud. Neither is the purpose of FedRAMP to assess just the minimum necessary controls for determining what is safe necessarily. The purpose of FedRAMP is to remove duplicative work. FedRAMP needs to be the maximum set of controls that could be done that cannot be that-- except for those that cannot be assessed, the hybrid control specific to agency's implementation. From where I'm sitting, the small agency are going to fight tooth and nail of reducing the controls necessary to receive a FedRAMP authorization unless NIST has removed that from a baseline, whatever low, medium high is. The purpose is save money from the Federal Government by not having to reauthorize the product over and over. What we end up is agencies have to do more work that is repetitive which is the whole reason we started this program, not stop doing that. I am going to scream and yell over this top I can, we cannot reduce the amount of controls that the FedRAMP team is responsible for. We can change how we talk about the controls. We can prioritize that are harder up the pipeline process. I am fine with all of that. I'm absolutely not going to be onboard with the notion of removing any of the controls. That's Mohr I'm going to do and have no budget. That's my overall statement. That impacts item two here. Again, I don't love the notion of like splitting this up. I don't love 6A as written. And again, I don't love 7 and around figure out 7C. Prioritizations is great for me, I don't want to remove anything. That's my big statement. Sorry, Bo, go ahead.

>> Thank you for that. Bo GSA. Just to be clear, the current FedRAMP baseline is built on top of the existing, 199 modern, high, baseline, adds controls on top. Controls on top, I should say I was there ten years ago in helping to define the initial control baselines, you know, for low, moderate high, representing GSA along with Kevin Delaney from DoD and the CISA from DHS.

The discussion was aligned to what was stimulated in the organization's cybersecurity policies. In the case of DoD, we require these things. These things need to be in the FedRAMP policy. DHS likewise and GSA likewise as well. Controls need to be specific to risks to commensurate with the association, types of service and sensitivity of what we're doing and what data we're exposing.

So you know, in that baseline it has positively moved forthwith additional controls over time that are Cloud specific. But what I will-- there are more controls in the NIST 153 catalog that are not selected in any baseline or inclusive in the FedRAMP baseline.

So if we wanted to go through and feel great about ourselves we should just go through and apply every control on the NIST baseline from the NIST catalog. But that's not what we do. There are a whole lot of controls in the NIST catalog that don't apply to low, moderate high, or not in the FedRAMP baselines themselves. All I've saying is we need to go through and make sure that we are looking at the controls to ensure that they are commensurate with risk associated with the types of information that are being exposed, and two, factoring cloud specific risks, environment specific risks and increasing I the risk we are facing with one Cloud Service provider stitched together with another to allow us to run workloads and micro services and container spaces and things of that nature.

There is an opportunity, so when Jacque said, hey we effectively look through the set of controls and actually removed some, I think that's a positive. Right? But these things need to be informed. We should go through and eliminate baselines and mandate every control from the catalog regardless of impact level which is something that we don't do.

And so for-- connect this in terms of going through and making FedRAMP more efficient in terms of cost, time, and barriers, there is a clear opportunity to have a risk based environment set of controls that are more appropriate. Over.

>>

>> Just to back and forth this a little bit. Again I'm generally onboard. The thing that I get queazy about is the second that we rule something that more than two agencies do and will be requiring on the other end to get to the ATO. The line is, are we or not removing duplicative work? It at controls no one cares about, fine. Anything duplicated and more than a couple of agencies will repeat the same process, that's going to slow down the ATO process.

>> I think we're on the same page, Bill. I will say it's for GSA, our role in government shared services. And we provide a whole lot of shared services and recently one of the projects we've been working on is a new federal travel solution for every agency, one solution for every agency. And you know what I did? I pulled NSA together, FBI together, DHS together, NIST as well as broad set of agencies. The first thing we did, we started with the FedRAMP baseline and did threat assessment, understanding what data, environment of operations, integrations, bids functions, user sets make sure we effectively appropriated the baseline to ensure that we were bringing to bear the rates of the controls. Why? Because exactly what you said what we did not want is individual agencies across the set, coming back and saying, I need this on top. I need that on top because that always is regressive, delays, and adds cost to our vendor partners that have to go through and re-factor additional control sets to pit agency versus agency.

There is an opportunity for us to go to make sure we are bringing to bear the right controls in a responsible manner and following step methodology that aligns the requirements that we have in the baselines to a set of requirements be a threat, be it data, be anything we expressed previously.

>> I agree.

>> Mike, you have your hand up?

>> Yeah, so I think what we were talking about in this section last time was the concept of a graduated technical readiness level. And so we talked on how NASA and this is NASA's TRL levels how they graduate up from basic technology research to allowing for democrats traces using non-production data up through system demonstration like qualification in this case all the way up to full board mission operating in systems.

And I think where we as an organization here are focused pretty much on the TRL9. We're saying CSPs to have fully realized system, and have it all of controls. We want the controls to apply to all data. I think we're losing the concept here that we can potentially do things earlier in earlier stages and allow the agencies to have access to systems earlier for mission development. Not using production data and not full controls but allowing you all to have access to systems earlier in the life cycle to build out missions so as CSPs bring us up to TRL9 readiness with all controls, you have the ability to say, yes, my mission is also available at the same time this new of have is fully qualified. That's what we were looking at in the past. I want to flip that out. That's the concept embedded in the ideas, in the document.

Again, it's wide open to interpretation if that's what we want to do or not. I want to make sure we have the right ones.

>> Thanks, Mike. Appreciate that. The next two hands up are Bill and Jacque.

>> I Filibustered it a lot. I'll let Jacque go ahead and come back.

>> Thanks, Bill. Jacque?

>> I was going to say, you know, it's an interesting concept. And I don't know, I'd throw this out just for thoughts is that, obviously a risk official has reviewed at an agency level that package before it actually goes into the FedRAMP review process. FedRAMP is that a place we as an organization or the Federal Government can take a calculated risk and let other entities reuse the artifacts and make their own reorganization--

So again, speed, this is a really huge place where I hear a lot of complaints which is the time it takes from an agency authorization to getting on the market place. They are losing substantial dollars from a business perspective. Is that a place where we can take risks to say that this has is a risk official has looked at this package, issued an authorization for an agency. And so can we take it and run while it finishes the last hurdles? I don't know how much scrutiny or how much rework is required from FedRAMP. I don't have any metrics there to know whether we have a lot of problems with packages that come before FedRAMP or whether this is a place where we can take risk. Over.

>> Back to you, Bill.

>> Yeah, talking about getting into this, I'm not oppose to the notion that each CIO should be able to set its own, their own acceptable level of risk for their agency and acceptance on a incomplete package. That's something that historically it doesn't lie with the CIO.

The problem for me is that in the new OMB memo they have said that you must have a FedRAMP authorization to use the Cloud provider's tool. A complete authorization. So by recommending this, I'm not sure that we would be in alignment with the OMB memoranda unless they want to review that where there was an exception process. They got rid of the exception process. They removed exactly what we're talking about right now. Intentional decision.

So they refuse to change that based on our recommendation. They have doubled down on it. I'm not saying it's necessarily a bad thing. I'm saying I'm getting queazy here because what we're saying what OMB said not to do in the memo. So that is something I'm stewing over, here. I want that exception process-- us small agencies need to do things faster. OMB has removed that path. That being removed, I worry about us recommending it.

>> Thanks, Bill. Marcy?

>> Thank you. For my orientation, what number are we on in these recommendations given this discussion here? Are we still on-- like two? I guess what I'm losing is how this discussion tied into the specific recommendations. And that was not my take away in reading this. It may have been perception on my side.

>> I think 6A and B are where we are.

>> Appreciate that. Just to pin onto this, the idea of agency making their decisions. That is why, when we talk about the FedRAMP PMOQ and the FedRAMP authorization that is granted by the PL. That's why the queue exists because they come there needs to be some sort of minimum. I don't like this term, minimum acceptable standard or baseline for what risk can exist. Is a decent starting point for reuse within the government.

And so that's why that FedRAMP authorization threshold exists. We're not relying on every single agency authorization granted. So yeah, that's all.

>> Thanks, Marcy. Bo?

>> I want to chime in to Bill's comment particularly reporter exceptions. He's absolutely right in that the exception clause was effectively removed. But what was added was other paths to authorizations. You know within the actual policy memo and I believe it's in section 4, if I remember. And I know we talked about as it relates to priority one. That might be a way for us to be able to take that and blend it into a broader recommendation, finding alternate paths to an authorized agencies to allow them to use the new technology, particularly focused on risk, especially lower risk. You can combine that with StateRAMP and other industry related certification from low risk-- you know, as for just the comment on Marcy's last comment as well, you we do have baselines for FedRAMP and low moderate high. But not everyone CSP needs every control. I've never seen one. Every CSP solution that is typically authorized from the provision authorization on agency authorization whatever that nomenclature is called these days, they are going to have some residual actions that they are managing through a plan of action milestone to effectively to get to a fully implemented statement

I don't know if there's one even that implements every control requirement. So identifying a common risk threshold, common risk rubric that provides some consistency around what controls would proceed conclude authorization? What controls and what conditions particularly those already authorized to operate would essentially go through and pull CSP provider out of a FedRAMP authorized state. I think that's incredibly important. And that's something that's actually been actively discussed through the FedRAMP board as well just to be able to go through and align some level of consistency especially as we are moving further with this joint authorization concept that is being piloted across.

>> Thanks, Bo. I think everyone's worn themselves out. Really robust discussion. Let's take a look at the problem statement in our recommendations particularly for this priority two.

See if we're getting close to consensus. I mean, recognizing, you know, Bill, your expression that you hate number two. That's, I mean, are you suggesting a deletion of number two? And we move number one from priority one to priority two. Are we okay with the way it's worded? I'm seeing things up. Marcy.

>> I agree with deletion of number two. I believe it exists. If the concept is to demonstrate CSP ability to get to FedRAMP status, have an implementation that would result in a successful authorization, that exists through the FedRAMP process. There's a lot this needs to be done. But I completely agree with Bill, this needs to be struck because I don't really agree with it but I also think it somewhat exists already.

>> Thank you. And I see Dan and Bill with thumbs up in the reactions. Thanks.

Any other edits on what's written in front of us? He

>> May I ask a question to Marcy real quick? Larry -- Marcy you probably have a good perspective on this given your viewpoint as a 3 PAO. How often do you see an organization issue an authorization versus one that is already FedRAMP authorized within the marketplace?

>> Good question. We would never consider ready to be an authorization. We often don't see the discreet agency authorizations that are being granted. That's not a process we are involved in. Beyond that initial sponsorship. Once they receive the FedRAMP authorization we don't see the reuse authorizations.

But what I am getting at from ready it's a FedRAMP ready status but demonstrate potential to be able to say, they've done the leg work and time and effort to produce a production system that is a good strategy to undergo that full authorization process. and achieve agency and full authorization.

>> I guess my question is, do you actually see scenarios where a CSP that you're working within support of a full assessment or in the advisory stages and having the FedRAMP ready package that, that FedRAMP ready package itself being used as some kind of internal agency authorization for allowing an organization to use while they work more broadly through the residual part of the FedRAMP operation process? Market entry?

>> Yeah, I don't know that we would see that as a 3 PAO. I can't say it's not happening. There were a lot of those risks and authorization decisions that happen at the agency that we're not privy to. I wish we were.

>> So the reason I'm asking this question is that, a GSA, for example, we have bridge authorizations for both moderate and low. You know, I've got a-- authorization that we issue based on subset of the FedRAMP low baseline to allow us to be able to quickly get to an operational state with Cloud service provider while we work with them through the residual set of the FedRAMP process to achieve a FedRAMP authorization and have that authorization be identified as authorizing FedRAMP marketplace. And we do the same thing for the moderate authorization or my-- stats authorization. All this to say that it allows us to be able to go through and achieve those authorizations and allow our agency to be able to leverage those technology solutions sooner on a risk basis while we're effectively working around some of the lower risk controls around awareness training and some associated controls that may not be directly at the highest level impact whether a CSP provider is going to have a secure and secure outcome.

So two, I think perhaps be reworded as oppose to going through and talking about it in the way that it is, i.e. splitting up the authorization process into smaller approval stages.

You know, it's not, I will say, a horrible recommendation because agencies like GSA I know are doing some element. What is being described here for themselves while a CSP provider achieves a full authorization. And worst yet some agencies use the CSP solutions without any due diligence whether a step up authorization or FedRAMP authorization.

>> That a recommendation? I guess is that a recommendation for the audience here? I'm trying to understand the thoughts, not a policy issue versus a FedRAMP program implementation.

>> Yeah, I think the policies, we want folks to effectively use secure vetted CSPs. That's the stance. That's what the FedRAMP policy advocates. But you know, having a capability or providing for a recommendation that more clearly signals to agencies, not to CSPs but agencies that there can be a step up type authorization program where you can go through and make an authorization decision for yourself based on your risk thresholds, based on, for example, a FedRAMP ready package, a package that has been submitted to the FedRAMP queue waiting in purgatory and waiting to go through to find and determine whether they meet the criteria to be added to the FedRAMP marketplace.

We should, and we can signal a recommendation to allow agencies to be able to do that. Some already do it. But the notion here, and it's just making that statement a little bit more explicit.

>> Sorry can I jump in Bo, and get you to clarify. Picking at that, what's the differentiator versus the other case we're talking about? It sounds like you're proposing a way for agencies to use things when the evaluations, quarter done, halfway done, three quarters of the way done, still right back if the statement place where each agency is responsible for the controls that have not been assessed or the pieces of the process remaining. With we saying, agencies will go faster and repeat the same work?

>> Not necessarily repeat the same work as much as to be able to go through, like in the FedRAMP category, for example, you've got 17, 18 control. You have A CIA, ACSI, technical controls that determine secure and insecure outcomes. Fed ramp readiness assessment the are focused on hardcore controls that are fundamental to secure outcomes.

So if you have a CSP that has completed the entire FedRAMP process, implemented the controls as work for the three-- and develop an assessment and authorization package and submitted that into the FedRAMP queue and now waiting for a year to be added into the FedRAMP marketplace, the package itself is a package that can essentially be used by agencies to allow them to make their risk decisions.

And some agencies already do that. Other agencies they basically have a signal, I'm not going to use it until that solution is clearly identified as FedRAMP authorizes in the FedRAMP marketplace. The notion is agencies are doing this. There might be a benefit to us to signal that as a possible recommendation over to the administrator to have the PMO work with OMB, work with the FedRAMP board to clearly tell agencies that you can use the FedRAMP in process package that has been fully documented, fully assessed and completed pending FedRAMP authorization, understanding the PMO is going to go through. And dot Is and cross Ts and make sure gaps are squared up.

>> I want to call on Mike. I saw Jacque with the thumbs up on your marks there, Bo. Mike's been waiting patiently.

>> Yeah, I wanted to definitely concur with you Bo. I think that's a wonderful idea and also we've seen in the CSP side of the house, we've seen specific agencies take a fed ramp ready package and put it to ATT rather than ATO, authorize to test and use test today data, non-production data. We've seen that before in some instances with agencies. It's not standardized, not across the board. And it is a kind of an at risk, low risk because it's not production data. But a risk approach that agencies allow. That would be something that would be, potentially be used in a formalized way across all FedRAMP agencies.

I did have another point. And I don't remember it now. If it comes back, I'll go.

>> Thanks, Mike. And Bill and Jacque?

>> Thanks. Bill SCC again. I generally like where Bo is taking this. I just want to make sure that we're careful in the language we end up having here in the final memo. I spent the last eight years to adopt the ATO-- that GSA has. I still think that GSA is more willing to take risks on this sort of stuff than most other Federal Agencies. Especially small ones for reasons a stated previously.

I think we have the necessary wiggle room in the me know if we read between the lines much the OMB memo says they must maintain (READING). Section 3. If doesn't say you have to have the authorization before you start using it which is a very, key piece of this. I would want to make sure we're clarifying with OMB that they're cool with us doing this whole round about way that we're proposing which is since they-- OMB doesn't have the authority to take away the risk acceptance from the CIO. They can't do anything about that.

They can't overrule that. So in theory the CIO can do whatever they want regardless of whether or not they have gone through the authorization process with the tool. They can use it. They're allowed.

I would want to make sure that OMB is willing to support this scheme that we have of saying, that halfway is good enough if agencies want to accept the risk and OMB is not going to like them through IG on us for doing this. That's the main thing for me. I would love for our agency adapt ATO, soft but not everyone is there yet. This would potentially be a way of making that go faster and spring it a along. I'm a massive proponent of that.

It's just a question of are we going to get slapped for it? That's what I'm worried about.

>> Thanks, Bill. Mike and Bo.

>> I want to add, this is one of CSP's number one complaint. To the points raised earlier, if we don't do something this this space and remove this priority, we're doing a major disservice not only to the FedRAMP as a whole. We're doing a disservice to all the CSPs large and small that are spending a costly amount of money to participate in this program and try to move things in the government space. So that the government can a large selection of services.

Ready available for all of your mission needs. So the more we limiter competition the more we raise the barrier to entry, the more we don't focus on authorization streamlining, but we're really doing a disservice to the community we're serving.

>> Thank you, Mike. Over. Bo?

>> Just to be clear, what I'm propositioning here is I would say, 50% of the way. Like in one scenario where a CSP has documented, implemented, assessed and submitted a package that is pending PMO review, I would argue that's 98% of the way through. And it's pending FedRAMP resource constraints in the PL level to be able to review PMO and really finalize the package of about entry the FedRAMP marketplace. That's proposition A.

The other proposition is what we do is our-- SaaS related processes a options, and you know, this is part of that step up authorization process. And that would probably be more accurate to call it 50% of the way through based on documentation and implementation, assessment much the most critical controls that are foundational to good or bad cybersecurity outcomes and allowing a one year authorization which is what we do. And then within that one year period we allow our agency to beginning to use on a risk basis with some conditions and within that one year period the CSP partner has to complete the control requirements, assessment, allowing us to be able to achieve that full authorization as originally intended.

Again, options, recommendations, kind of think outside the box how we can go through and run faster. Over.

>> Thanks, Bo. Next two hands up are Jacque and Marcy.

>> Sorry I was going to get back to the wording. And so in the item one, I would suggest and I wouldn't type until we get the people's thoughts on this. Reducing the time to authorization and use. And then adding a C which is the FedRAMP PMO will engage OMB not task, we're going to engage, don't want to step on any toes here, to clarify when a CSO can be used and EG when it enters the FedRAMP PMO queue for review after agency authorization. I think that's what I've been hearing from everybody. I just want to put something down on paper, see if we could take other tasks.

>> Thanks. Appreciate that. I think Marcy is next and then Bo you have a hand up.

>> Just kidding. I will lower my hand because Jacque offered the clarification. Thank you.

>> I appreciate that very much. And Jacque, yes, thank you. Bo?

>> I just forgot to take it down.

>> That's all right. So Jacque, thank you for that and for bringing our focus back to the wording.

Fantastic discussion. And you know, great clarification on the concepts. And so to now translate that into actually coming to consensus on the wording if we can in the next 22 minutes on priority two, I'd love to be able to accomplish that.

So and in that and with that, on the action an recommendations, we can't send all eight, I think that we have here now, eight, yeah. So we're going to have to pick the top three of the eight. So it's possibly in the next 20 minutes or so, coming to consensus on the wording of the top three. First of all, picking the top three most impactful, most important. And we deleted one by consensus. I appreciate that, everybody.

So are we ready to do that? I'm seeing hands now from Bill, Marcy, and Jacque. Great let's start with Bill.

>> I'm trying to keep track of all the renumbering. But I believe five and six can likely be condensed into a single one. We're saying the same thing two different ways. It sounds like it's addressing the baseline authorizations and having a tiered system of some sort as Bill was describing. From where I'm sitting we can somehow word Smith those two into one. I would guess if I'm reading this right.

>> I think it's three and four. These two, right?

>> On the screen in front of you, Bill?

>> I have the same thought.

>> I think three, four, five and six are basically the same thing reading this again. Right? We're say what's in the box, what's not in the box, when you can and not use it. Is this not one version of the same thing

>> I would put 5 with 1C where we landed. That's looking at the step process of when a product can be used.

>> Yeah, I concur with that.

>> Let's do that. Put five with 1C.

>> I'm going to implore my colleagues here for whatever the last one now is numbered, the exploring and establishing financial support and incentives. Whatever that is, this remains the absolute most important thing that continues to slip through the cracks. I would implore everyone, this absolutely needs to be one of the most important things. Others are fun, I love them realistically we need to find other ways of getting money out there for people to do this stuff.

>> Marcy?

>> I concur Bill's statement here. We have combined three and four just to confirm if we can do that. I think these are two sides of the same coin. And move that up. And bill's points to financial impact. I want to go back to PAO's suggestion was note knots look looking tout out of the box for cost recovery, charging a fee for authorization at certain stages of the authorization process.

StateRAMP does that now. That exists in a complimentary model. And I will anecdotally say we have had requests from various CSPs asking in the context of pay to play. Is there an opportunity for us to pay money to go faster? I think the appetite is there.

>> Cool. Can I directly respond to that and say that is a huge advantage to the big players and huge advantage to small businesses.

>> I agree.

>> That is extremely problematic for me. I do not love the StateRAMP model of pay to play. I don't like the Federal Government charging people to show up at the door. It makes me queazy.

>> Bill, I hear you and have the same hesitations. If that is applied consistently or done at a tiered, does that change your appetite on that at all?

>> I mean again it costs money to run the program. But at the end of the day it needs to be authorized centrally from Congress. They believed in this enough to write a law about it. Then the least they can do is fund it. Right? Like that's kind of where I'm at. If this is really important, appropriations needs to talk to the other committees.

>> Do we recommend them to the administer that GSA locally for increased appropriations?

>> Well, legally you're not allowed to lobby. So let's not use that word. But I think we do say in here that explore-- discussions supported by Congress for additional ways of funding this. I strongly endorse that. We talked about using SBA for the businesses but in general agencies need money for this to work. Aside from the word lobby, I'm okay with that.

>> thank you for checking on that. Does the committee want number five to be number one?

>> I would support that.

>> I would supported that, too.

>> Put money first. Jacque has her hand up. Jacque while we're doing that, calling on you.

>> Be careful what you ask for. I will say that at one point GSA approached DoD and was going to tax DoD to pay GSA. Time out, I'm limping along here. And now you're requiring DoD to spay to support FedRAMP. Anyway, I don't-- I'm aligned with Bill. I don't support charging the Cloud providers more money. They are paying the 3 PAO, the cost to enter is expensive and comply with all the art facts and continuous monitoring and the requirements we have is steep especially for small businesses.

On an agency side it is very expensive to do the-- but what I think we've got to hear from FedRAMP to figure out where they are in automation process. And that is going to be lower some of the tail toss that we have in terms of (?). I got a note from Marcy to look at participating on a pilot on con (?). You started this particular section with, you know, whereby do we go from here? How do we whittling this down?

I would like to hear from FedRAMP which you said is going to occur in our next meeting as to what they see would be helpful for them to move the program forward?

You know, I had a discussion and it was like, you know, the recommendations aren't really helping us because you're stating the obvious and things we're working on. So I would like to hear what they would find helpful and use that to craft some of our recommendations as we move this forward. I'm not saying they're driving what we do. But I want to know that we are helping move this ball down the road and getting some of these things addressed in a timely manner and not duplicating or stating things that they already have in progress or close to crossing the finish line. Over.

>> Thanks, Jacque. Appreciate that. Kayla and then Bo.

>> So I love, one, I love one. I wonder if that should be the first recommendation for our first priority which is barrier to entry is a small business' ability to afford, to pay for the, for getting started in this. Is that a barrier to entry? Or is it going to expedite their authorization process?

So it's kind of I guess, my question to the group. I think it should stay absolutely and should be a top priority. But does this make it more feasible for small businesses to wet into FedRAMP or does it make FedRAMP authorization process faster and easier? I know we have cost tied into priority two as well. But I want to throw that out there.

>> And Bill's indicated a thumbs up. Bo and Marcy have happens up. Kayla, I don't want to lose your thread on that but let's go to Bo and Marcy.

>> Just on this cost sharing incentive idea, I think the suggestion here is not to make that formal in a way that everybody has to effectively go through and feed FedRAMP. Right? But rather make it an option. And in the same way as Matt was talking about and that certain CSPs if they want to get expedited you can pay. This could essentially be an inlet to create for that supply that we need both from the PMO standpoint as well as from the agency sponsorship level.

I wouldn't go through and make that some kind of a hard requirement because at that point, Kayla's right. It's going to be another barrier. And we're basically adding to the problem set as oppose to getting through and alleviating it.

Identifying that as an option that they can go through if they want to speed up through the program and process. This comes down to dollars and cents issue if you're a CSPs because time and delay is itself costing them their significant amounts of money because they've invested significant sums to be able to go through and achieve a FedRAMP authorization. And then they're waiting. They have invested significant amounts of money to achieve a FedRAMP authorization and the very technology that isn't waiting is actually regressing as the environment changes.

And so being able to go flu and capitalize on this through an incentive or cost sharing model at their option might make sense.

>> Thanks, Bo. Bill, you're next.

>> How do we do that without just the big vendors going and taking in all the slots. Right? Again, I'm happy to consider this concept. But at the end of the day it just means the big three by all the priority over and over again to the define sit of all of the small businesses. That's the thing I'm trying to avoid. Small visitors are not going to afford going through. They don't have the money for that. They barely have the money for assessment. How can we do that in a way a that's equitable and leveled playing field rather than deepening the divide.

How many of you have been to Disneyworld and have the special wristband. Those people are jerks. I hate those people. Those of us who can't do the overnight, that's annoying seeing those people at the front of the line. Again as a previous small business owner, I don't love it.

I understand the need, but there's got to be a better way than expecting us to compete with the big three. That's not realistic.

>> I lost track of who is next. Kayla is on the screen--

>> Kayla first.

>> Okay, I also want to throw in there with the, I think even a small or medium size business, there's this carrot if I pay to help expedite the process, I mean, agreed with your comment of time is money. The longer this thing waits, the package waits to be approved, that's wasting my money. So maybe it's worth it to pay for things to be expedited. My thing is, what's the guarantee that that is going to be expedited? How much of our challenges are, how much of the challenges that face, that make this ATO process long are due to pure money constraints?

I heard comments about talent constraints and documentation. Money can fix most problems. But how much of this is beyond just I am here to pay to play and what's my guarantee that that is actually going to be expedited? And what does it mean? Six months versus 12 months or one year versus two years. I know we don't have the details. We're discussing the idea in general. As a small business CSP I would want to truly understand that pay to play or that incentive for expediting is going to be actually beneficial for me.

>> Thanks, Kayla. Now it's your turn, Bo.

>> So just to clarify. I think the idea around cost sharing was really to induce or entice sponsorship because what we had talked about as a barrier of entry was CSPs willing, able to commit to FedRAMP but not finding a sponsor.

And we said that the challenge was that agencies Bill himself said that agencies didn't have the resources to be equitable to sponsor. The expedite came from Matt suggesting that the validation process also had, you can pay a little bit more to get faster through the process. I think we shouldn't confuse the expedite via sponsorship and allow cost sharing model.

I should tell you at GSA, I've got a small team. And I go through and charge my business owners like Larry -- for example, who wants to use a-- CSPs solution that's going to be a game changer for business opportunity. I go to him and say, you're not CSP authorized, you have a need. You give me-- cash and I will work there you that CSP solution and sponsor them. And I have a cost model for a low system, moderate system, high system. I'm sure Jacque and others sponsorship also have a cost model. Maybe it's centralized or fee for service. The notion here is, when I go to our Program Managers, they're centrally budgeted only a specific level. And usually they don't have money to give me. So they have to either find the money or we're in an impasse. So that's the basic idea is not necessarily to further entice or induce quickly their process but really around cost sharing to make easier for agencies to say yes to sponsorship. Over.

>> Thanks, Bo. Next up is Bill and Matt and Jacque.

>> Bill here. The more I talk about this, the queasier I'm getting. Now we're getting into all weird of ethical territory.

Like people are paying to play to get in the door at the agency. We've got a whole lot of ethics rules designed to not do that thing. So we're shredding into dark waters. We're talking about getting to the somethings sponsorship part. If the big vendors are paying, everybody else slows down and that means the process gets more painful for the small businesses that can't compete because all of the speed is taken up by the people who have the money.

Honestly a lot of that is happening beyond closed doors. Big vendors can get the package shaped up and check boxes checked. They already have the expedited path. So again, I don't love money and politics. I'll say that. I'm not feeling good about this one.

>> Matt?

>> I love money and politics. So in case I wasn't clear earlier, I'm sorry if I wasn't

The crypto module value education program, FIPS, does not have an expedited payment process. What I was referring to was the Food and Drug Administration has one for some of their medical device. And adverse effect drug review processes. So what I was saying, there are some agencies who do the same program does not.

The other thing I think we're making a lot of assumptions about is what the model would be. So if we want to keep this, we can abstract this up to explore the feasibility of financial support or incentive programs, putting in some of the guardrail outcomes that Bill stated around things liken suring fairness, equity, and accessibility of all participants. And then if it turns out it's not feasible, then it's not. At least we can look at it. I'm sure Marcy would like this. What we do in the CMVP program, we don't charge the vendors. I charge the test labs. And the test labs have an annual fee that gets them, amortized across the customers. That allows the market to make decisions about what people can or cannot afford and who they engage for their testing partners.

I don't know if that's feasible in this model or not because it's not a straight one to one. But I just say that to say, you know, let's not make assumptions how it potentially would happen. Let's roll it out as let's explore and see what's potential and not potential.

>> Jacque?

>> Let's say, I do not have a cost reimbursable model. Department, so you understand how we do business. We are an appropriated activity. So we have appropriated dollars that pays for our government entities and the contractors. One of the things we do is all of our DoD components they have to sponsor what they need. And they have to put skin in the game, and the skin in the game is they have to provide depending on the scope of the assessment, whether it's a star from are control zero or up lift, they have to put in two to three validators or our team to assist and we lead the activity. That is how we have addressed resource shortages that we have just because the appropriation is insufficient for the scope of the work that we are now doing. But we do not have any cost reimbursement on our end. And we do, in our secret cloud, we are doing our own red team assessments, for example.

And so we've got a lot of different ways that we're trying to tackle this, but it is not from a reimbursable activity. Over.

>> I'm sorry to jump in. Jacque, that's an excellent point. Maybe feasibility of financial and resource support and not limited to financial.

>> So thanks, everybody. We are just about an hour deliberation on this. Does anyone have any additional comments or recommendations they'd like to add to either priorities? These are just our initial plots because nothing is final until we vote on the final version. We will do that, vote on the fill recommendations at a future meeting. Jumping between the screens to see if another hand is coming up.

Okay, I have one small ask. We had a lot of viewpoints around the cost sharing idea.

Would each of you commit to brainstorming on your own time on what a potential cost sharing model may look or not look like. Taking ethics into account. And bring your ideas to the next meeting. I'd love to get everyone's commitment on that.

Thanks, everyone.

If there's nothing else on this, I'll pass it back to you, Michelle. And thank you, all.

>> Thank you so much. I appreciate it. Thanks, Larry. We've reached the final topic for our agenda. I will pass it back to Larry to discuss the next steps and provide the closing remarks.

>> All right. I am off mute. Okay. So again, I want to thank, fantastic discussion. I want to thank you all for your active participation today. It's been a robust discussion on the first two priorities and I look forward to continuing to work on our next set of priorities in our next meeting. We have to finish these up as well.

Before closing today, we have captured the summary of next steps from the last meeting specifically we said that we like to have Pete join us again with update on FedRAMP and that we want to move forward and request public comments once we have our LinkedIn account set up.

Today I want to ask the committee again if there's any information gaps that would further, would require further information or clarification for these two priorities? Are there initial specific speakers or stakeholder panels that we would like to hear from?

>> Hey, Larry? I know Bronco's not here. Something he mentioned last time is someone stepping through the entire process flow. From initiation through authorization so that clarity on issue points or opportunities would be or could be identified. That could be part of the FedRAMP ask for their talk.

>> thanks Matt. Bill?

>> As far as priority four, I'm going to be first to admit it's been three years since I had direct work on the program since my time working on that-- so I would be curious to hear the current state of the world of OSCAL, what's in play and tools provided. Anybody implemented it from the-- from that side in addition to from the government side. Again I think we all know I'm a huge fan of OSCAL. But I will admit I am out of date as to what the current state of play is. Would love to hear from the vendor community using it today as well as the programs on that one.

>> Thanks, Bill. Yeah, big request. Mic?

>> Pete came in and spoke at the summit. And so-- (audio breaking up). About asking CSPs to engage and lean in with resourcing to help move the FedRAMP program forward. There's been ask from the CSPs as to refining that into some concrete actions that they can help participate in. So I'd love to see that. And I'd love to see potentially a roadmap or progress update from the 2023 priorities that we provided to FedRAMP PMO last year. I see it up there. Cool.

>> Awesome. Thanks, Mike. Jacque?

>> Current state of OSCAL, I'd like to here from a 3 PAO as well. If we don't have 3 PAO with the tool, actually able to capture all of the results of audit to pull into our GRC, if we don't have that side of the house, if we don't have a SAP and OSCAL, this is a robust end-to-end, where are we-- I'm glad Bill brought that up. That is something that I'd like to hear. Is it comprehensive enough and do we have the tools in place or still in the theory stage of OSCAL?

>> Thanks, Jacque. Yeah. So essentially service provider slide, government slide, 3 PAO side and OSCAL panel with those three. Thank you.

All right. Thank you all. So with the last few minutes that we have, I also want to give Bo the floor for a minute as he has some news to share with us. So Bo, over to you.

>> Thank you, Larry. You know, I just want to go through and take a minute what an honor and privilege it has been working on this committee. Tomorrow is my last day at GSA and last day in government. I'm transitioning out. And going on wards to industry and working at a small nonprofit. I'm still focused around public service and advancing the mission of public service in a new capacity.

And you know, it's been such a pleasure alongside such talented and dedicated team of members on this committee. Truly a privilege for me. I think work at this committee is critical to advance the security adoption of removing the barrier entries CSP. We've been talking about today, that has really been the foundational-- I hope that the work we're doing has a positive impact in helping to address the underlying challenges our CSP partners and Federal Agencies in advancing their missions that benefit is realized. Larry I want to say thank you to you and to your predecessor Anne Louis. Michelle study for your stewardship of this committee. This doesn't happen with all of the back end staff that make this possible.

So my hats off to all of you. Really enjoyed my time on the committee. And I'll continue to find new ways to be able to contribute positively to the important mission of FedRAMP. This is something I've been effectively engaged in since the very start of the FedRAMP program and the work we had done originally led up to the actual foundation of the FedRAMP program.

So it's incredibly important to me and I'm really ecstatic to see that we're sitting here, talking about how do move this program and make it successful for our stakeholders and community.

Thank you for all of your time. Thank you for all of your continued support and attention to this really vital program not just for government but for our nation because the critical services that we use touch almost every member of the American public.

>> Thank you so much, Bo. You will be missed. We really do appreciate your, especially what you brought to this group and the knowledge and even today. Your second to last day in government, you didn't sit back and mute. You engaged and leaned forward. You contributed meaningfully and passionately. We're going to miss you. We appreciate you very much. And wish you the best in your new adventures.

>> Thanks. We appreciate you. And also we'll be replacing you with an AI CHAT BOT.

>> You didn't say AI then the wail way you said it first time earlier in the meeting. There was-- this was a sweeter way of saying AI. Thank you.

>> Bill, just to let you know, I am building an AI BOT within our organization. So if you're interested, you can reach out to my deputy. Large language model that helps to go through and really train on federal laws, OMB policies, NIST, everything. And eventually once we have it authorized to operate, much of our own code and related documentation to help our teams to facilitate, the important work of the assessment authorization and the other bevy of security related work actions.

>> Awesome. You know my passion and interest for this in the general area. Put I can't afford the rate. But happy to dish out about the work you're doing.

>> You know when you're gone it's going to be renamed the Bo BOT.

>> Indeed.

>> I don't know that, I just made that up. But anyway, Bo, thank you so much.

For the rest of the committee, as this is our last meeting of the new year, I want to thank you all again for sharing thoughts and participating throughout this year. We've had so many great discussions and narrowed down areas where we can recommend improvements for CSP in the government. And I look forward to delivering the report to the administrator in the new year. As always, please re-read and take note of one, comments they are helpful. I love the way the latest public comments fell right into the discussions today and informed them. And that's exactly what they're there for. In the meantime I look forward to our next meeting. Thank you for your diligent and thoughtful work. If it's not too early to say so, Happy Thanksgiving, happy holiday season and Happy New Year. Michelle, turning it back to you.

>> Thank you for joining this meeting today. With that I will adjourn the meeting at this time. Thank you all.

>> Thanks, everybody.