[Job number 7444235]

[Federal Secure Cloud Advisory Committee October 2024 Meeting ]

[ 10.03.2024]

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.

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

1

Test test test.

[Captioner standing by].

>>MICHELLE WHITE: Good afternoon everyone we will give everyone

a minute or so to logon.

[Recording in progress].

>>MICHELLE WHITE: All right good afternoon welcome to the

October 3, 2024, meeting of the federal secure cloud of the advisory

committee my name is Michelle White I am the DFO for this advisory

committee.

I would like to thank all of our presenters attendees and

stakeholders for joining us today including those who provided public

comments.

Public comments submitted via the for his cat public font comic

form by Wednesday, September 25th have been provided to the committee

members.

Or restart there are a few things that you should know. This

meeting is being recorded via zoom. This is an advisory committee

that is statutorily required under the James M half national defense

(inaudible) .

This formally establishes the federal advisory (inaudible)

the very 28th 2023. This committee is considered a federal advisory

committee it is governed by the requirements under factor.

My role as the DFO is to manage the day-to-day administered of

operations of the committee, attend all committee meetings and ensure

the committee operates in compliance with backup.

The duties of this committee include providing advice and

recommendations to the GSA administrator.

The board and agencies on technical financial programmatic and

operational matters regarding this secure adoption of cloud computing

processes and servers.

(Inaudible) specifically it is to examine operations

(inaudible) clicked information feedback on agency compliant and

implementation of requirements.

(Inaudible) I will now go through a role call for all of the

committee members please let me know you are present by stating here

is Larry Hale?

2

>> Here.

>>MICHELLE WHITE: Michael your circa? Colton Harris? Kayla under

Koffler? Josh Kruger?

>> Here.

>>MICHELLE WHITE: Daniel Payne Marcy Womack.

>> Here.

>>MICHELLE WHITE: C1 bronco broken (inaudible) Bo Broyles

(inaudible) Naaman on sorry Bill Hunt and Joshua Cohen? Thank you

all it does look like we have a quorum established.

I would like to go over the purpose of today's meeting it is

twofold. We want to agree on the structure of the phase Report.

To the administrator and begin drafting an initial set of

recommendations for the committee's first two priorities.

The intended outcomes for today are to have an agreement on the

report structure and a document (inaudible) draft report.

Our agenda today is as follows. Welcome and call to order to

take place from noon to 1210 and then we will jump straight into our

public comment until 1230.

And then some quick chair remarks until 1235 next we will dive

into our first discussion on the report structure until 105 followed

by a short ten-minute break until 115.

Following the break we will spend the rest of the meeting

discussing the committee's individual discovery and drafting initial

recommendations.

Which you capture life in the report template. Finally, we will

in the meeting no later than 3 o'clock by sharing next steps.

And closing remarks. If at any point we have an agenda and an

agenda item early and are ahead of schedule we will go on to the next

title (inaudible)

A few housekeeping items for our committee members and speakers

today. Please be sure to identify yourself before speaking so those

listening online are reading the minutes afterwards can know who made

which comment.

This is a virtual meeting please make sure that your microphone

is muted anytime you're not speaking. When it is time for the

committee to deliberate and you would like to raise your hand.

3

Please click on the reactions button in your menu bar and then

click raise your hand.

And remember to lower your hand when you're done speaking last

if you are not a committee member please hold all your comments until

the public comment.

And again please ensure your microphone is on you otherwise.

Let's move on to our public comment.

Our agenda today at the time we would like to welcome members of

the public to share the common story speakers please note a timer

will display.

On the screen indicating a time remaining and it will indicate

that you are out of time. Each speakers allotted four minutes to make

the comments.

We will be interrupting comments speakers who exceed four

minutes. So please speak sufficiently and please be respectful of the

time.

As a reminder a public comments a minute by Wednesday,

September 25th were presented to the committee members prior to the

meeting.

Went that let's get started. As a quick recap our producer will

take us to our public website to show us where the public comments

that we received so far

We persist we have received a few comments I will begin by

calling on those who submitted comments on mining case they are in

attendance today.

I would like to elaborate further in this meeting. Colin

Whitlatch would you like to speak? How about Scott Beauregard?

All right, well if anyone else would like to speak today please

raise your hand and I will call on you in the order that you have

raise your hand.

All right it does appear that we do not have any comments

public comments for today.

So with that we will go ahead include our public comment

section for today thank you all.

We will now transition to our first item chair and remarks

welcome Larry is the committee chair I will invite you to make any

opening remarks at this time.

4

I will be happy to answer any related questions that should come

up.

>>LARRY HALE: Thank you Michelle. I would like to provide a

brief recap of our priorities and what we covered during our last

meeting and then set the stage for our meeting today. If I can move

there we go.

As you all know during our July meeting we further refined our

top priorities and decided to begin developing recommendations for

these first two listed on the slide.

I will give everyone a minute to reread these. We were also

given to additional priorities from the GSA administrator. We agreed

to address them.

After working on these two initial priorities first so our work

today will be focused on these two priorities during our last meeting

on September 12th we heard from OMB.

On the federal policy memo and its impact gain a better

understanding of the challenges stakeholders face during the said

ramp authorization process and received excellent feedback from both

industry and agency liaisons.

On our top two priorities of the year. We also agreed to

complete our own individual research while awaiting and working on a

new social media account.

Today we will agree on the structure for our report and then

begin documenting our initial recommendations in the draft report.

Please note today's overall purpose is to begin drafting a report.

Nothing on the report is final until we hold an official vote. I

encourage all of you to speak up with any key information or initial

recommendations you would like to propose.

The formal the will of course take place at a later date to

ensure there is a dedicated time for thorough deliberations.

What questions this committee have? And remember please use the

raised hand feature in zoom. To begin to address your questions.

I know I do not need to tell this committee to not be shy while

you are thinking about the two priorities and any questions you may

have me just give you an update.

On our social media status that I mentioned earlier. Phase CAC

staff are still working on getting a LinkedIn account set up and hope

to have more information in our next meeting on the status of that so

5

if there are no questions.

I will pause for another minute and then jump into her next item

for today. So as I just stated we are going to determine our proposed

report structure.

So let's review the proposed report structure that the phase CAC

staff have drafted for us and determine if there's anything we would

like to change or modify.

In order to reach agreement on the structure. As you can see

the producer has brought up the structure in front of us.

On the screen this draft report was sent to committee members

last Thursday, September 26th for your initial review. The structure

is based on what was used for the last report to the minister.

After having reviewed and reflected on the previous process of

drafting a committee report before does anyone on the committee have

requests for changes or modifications?

To the proposed report structure? Since I know this is not a

shy group and I do not see any hands coming up and nothing has been

typed into the chat.

I am going to assume that based on having received this on

Thursday, September 26th you conducted your initial reviews that the

committee agrees on the basic structure.

Let me just ask once again if there is anyone here cannot live

with this report structure again it is a replica of the structure we

use last year.

If there's anyone here who cannot live without report structure

please indicate so by raising your hand now.

>>MICHELLE WHITE: Larry it looks like Michael has his hand

raised.

>>MICHELLE WHITE: Great. Michael.

>>MICHAEL VACIRCA: This is Michael representative called service

provider should I just had a quick question on the actionable

specific recommendations.

In that section is that where we would see potential metrics and

metric thresholds as something that we would (inaudible) .

>>LARRY HALE: Certainly if the committee if in a recommendations

if we want to propose metrics that would be the place where they

would be. Michelle and my making a false assumption?

>>MICHELLE WHITE: Nope I completely agree with you Larry. Mike.

>>LARRY HALE: Mike thank you for that clarifying question yes if

the committee proposes metrics with the recommendations this is where

6

they go in the report. Any additional questions?

>>MICHELLE WHITE: (Inaudible) has her hand raised also.

>>MARCI WOMACK: Hi thank you Marcy will make a shaman. We had

some discussion within the last deliverable about kind of additional

commentary.

To support some of the assistant summarization or more things

here this is an open question is there merit to us having an

opportunity to add additional commentary.

Or context to some of these recommendations? I personally would

lean toward yes at the risk of bogging down the document because I

think sometimes that might be important for the recommendations but

just wanted to ask about that?

>>LARRY HALE: I believe so and I think that the committee notes

may be the place to do that but yes I think we need to be as clear

while being concise.

I do think we need to be as clear about our intentions and her

concerns so I would say yes.

>>MARCI WOMACK: Again I apologize I miss in on my gosh I'm sorry

to cut you off Michelle.

>>MICHELLE WHITE: No worries what I was going to state is in our

deliverable on the OMB memo recommendations to the GSA administrator.

We did have an appendix that we attached with some additional

information we could do a similar type of action with this document

to.

>>LARRY HALE: I like that. Because there is some stuff we may

want to put in committee notes but if we need to go further and

amplify deeper we could put that in an appendix.

We definitely want to be clear I mean that is the thing we want

the product of this committee to be clear and actionable. Anything we

can do to help clarify I think that is appropriate and welcome.

Other hands? So, once again just to validate as a basic

structure for the report when we do actually draft the report I

including that we have consensus agreement on the structure?

Again if you cannot live with the structure please raise your

hand now Michelle? Ready to move next item?

>>MICHELLE WHITE: All right yeah sounds great I will say the

next item was break so we can have go ahead and skip that right now

move on to our next item.

Which is starting the deliberations we can potentially take a

break during the deliberations portion basically going to be moving

on to the deliberation of the initial drafting of the report so Larry

back to you on doing the deliberations.

7

>>LARRY HALE: Absolutely and thank you Michelle. Committee

members, we have agreed upon structure for the report and as Michelle

said now it is time to go ahead and start entering our initial

thoughts and recommendations that we would like to highlight for the

administrator.

To ensure we address both priorities today I propose we time

box these deliberations bid we are little bit ahead of time but let's

spend not more than 45 minutes on each priority.

So 45 minutes on the first and move on to the next priority for

about 45 minutes and that will leave us with some time for additional

comments at the end.

So if this CAC stack please ensure to keep an eye on the clock

for us today with that let's dive in. You receive some additional

notes for members who are unable to attend today.

So let's review those quickly and also see if anybody has

anything they would like to add to these. These notes are about to

be shared on the screen.

>> (Inaudible) .

>>LARRY HALE: We are still seeing the structure the graph

recommendations unless that is what you have and committee notes that

is okay.

These are the notes we received in advance of today's meeting.

Which I misread as part of the structure but I think we will include

in part of the structure anyway.

Again folks we got a couple comments from Kayla that we want to

share give you time to read those.

>> I just have a quick question (inaudible) could we make it

so we can actually see the priority as well as the notes on the

screen? Perfect, thank you.

>>LARRY HALE: All right looking at the first priority identify

publicly document check top challenges impose solutions around the

barrier.

Does anyone on the committee have initial thoughts having looked

at Kayla's recommendation? Initial thoughts on the problem statement

a recommendation?

>>MICHELLE WHITE: (Inaudible) she had her hand up or is it just

left up from last time?

>>MICHAEL VACIRCA: I will actually will take a little bit. I

think just from the problem statement to start with I think a little

8

bit of clarity around barriers of entry to make sure we all

understand this includes financial technical compliance and

operation.

Of rate operational barriers (inaudible) so we clearly defined

that. Cost resource availability regulatory complexity those are all

the things that we are focused on.

I could throw that in this I chat to if we need to copy and

paste that into the notes but that is I think having clarity on a

Mike would help a lot.

Everyone is the impact on innovation so highlighting how these

barriers may be stifling innovation and competition what basically

what is the outcome of the current state?

So just emphasizing that there is high cost and complexity in

the complaint space. And it is limiting participation.

Especially from small business think is going to be something

that we should hit on the problem statement or derivation of the

problem statement.

>>LARRY HALE: Thank you Michael.

>>MICHELLE WHITE: And Bill you have your hands up?

>>BILL HUNT: Hi everybody Bill Hunt SEC one thing that came up

that I found interesting in the last meeting that I had not

considered before was specifically to the resources tier.

The bottle next of the three PALs not having enough staff

basically to be even be able to respond not having enough three PO

around I guess. It's kind of no seeing that.

I do not have a really good answer for that. But to me it is

the first time I'd heard it in that context but repeatedly my few

folks.

That to me just sounded interesting and I see Marcy has raised

her hands on eager to hear what she is going to say about that. I do

not want to spend a lot of time picking apart everything that

everybody has arty said here.

I will say that Kayla's note, documentation burden I think is

very real but I do not know the specific and actionable way of

resolving that.

Because there really documentation is the main point of this

exercise that is what we're doing here so you either get

documentation or you get off scale.

9

Is really the only two approaches we have and are talking about

specific and actual solutions I think that seeing reduce the

documentation is not sufficient to be specific and actionable

homeless people have other recommendations (inaudible) .

That would be my concern with that. I will cede the floor.

>>MICHELLE WHITE: Marsico had thank you.

>>MARCI WOMACK: You think you this is Marcy just add on I would

add anecdotally I would argue that it is not a three PO bottle neck.

Aside from not there is an issue with like time to get through

the authorization process for CSP's. All of the things that

(inaudible) .

There are phantom requirements things that do not come up until

the very end and someone three PA owes know about it because they go

through this process day in and day out and some may not it is often.

Increasing transparency within the Fed ramp program publicly is

going to be very important in the speed at which there documentation

guidance etc. Is published is very critical to making Fed ramp more

accessible.

And allowing CSP's to realize the financial benefits of federal

authorization faster knowing how much commitment goes into that to

get to that.

>>BILL HUNT: Sorry Marcy can we engage in some (inaudible) our

expert witnesses told us there was a three PO bottleneck.

>>MARCI WOMACK: I hear you and I do not want to deliberate on

that too much mostly because we personally do not find that there is.

If you examples we have organizations come to us.

And say hey we need to go through this right now. That is always

too late to start trying to engage in external assessor for literally

anything.

Also I would argue that there are a lot of organizations not

want to start right now I want to start in February and they are not

ready.

They start they do not have all the things in place that it

takes to complete the process successfully I do not know if there's a

ton of minutes to argue that but we do not find that three PAO

capacity is a significant issue.

>>BILL HUNT: Again I will defer but isn't what we heard

necessarily but you always experience I also have infinite respect

for I will definitely double down on.

The other thing you sent out with people not being ready I think

10

we heard Tom said that in Alaska as well. Folks just not knowing even

what the processes supposed to involve her look (inaudible) I

strongly agree with what you said on that.

>>MARCI WOMACK: I want to be in terms there are certain

improvements that can be made on the three PO side it is pretty

heavy-handed in terms of the number of authorizations.

Are number of assessments performed or authorization select the

top four to 53 PAO is kind of on the marketplace if you do that sort

that's pretty apparent.

I think there's additional work that can be done to ensure that

many other three PAO's have the right information and have experience

with handling the PMO discussions etc.

Thank you.

>>MICHELLE WHITE: Great Josh go ahead.

>>JOSH KRUEGER: Afternoon Josh Kruger project host. One of the

hardest parts it seems like to get a Fed ramp authorization if you

have all the paperwork in mind (inaudible) .

Is finding the agency sponsor and the agencies answers the only

way to get authorize right now. So part of it is the agencies just do

not have the resources to jump on board to review these packages at

the level they need.

To issue the ETO so is there something we can do to simplify I

guess the ETO work for the agency. I don't know the S PC

documentation like Marcy said people just don't know they are not

ready they think they are.

But is it the agency really needs to review the CIS

(inaudible) they need to review this are has the finance from the

three PO assessment with the vulnerabilities get a good rest of the

picture.

Of the package do they really need to read through 500 pages of

SSP's to see what the CSP is doing for each individual set? Probably

not but it is adding weeks months worth of work for these agencies.

Is there some type of modification doing million different

presentations for the agencies kickoff briefs to make sure they

understand the authorization boundary. (Inaudible)

How can we enable agencies to issue ETO's and save them from

excess reviews I guess. Do people not see it as excess? And then just

the upfront cost that CSP's have to do when you have a year-long

18-month long process.

To get authorize a think that is part of the problem statement

11

to smaller CSP's they do not have the upfront capital to pay for

consultants retrofit the environment to be compliant building

environments be compliant.

Higher this three PO often no initial investment from the

agencies right? Until they are authorized and under contract.

>>LARRY HALE: I'd say you definitely hit on something Josh could

you had a lot of hands raised up to start proposing this.

Is going to mention it is related to what Taylor recommended as

well in her first know but let's move on to the next hand.

>>MICHELLE WHITE: Great Daniel go ahead.

>>DANIEL PANE: Is actually to say this is Daniel from data

breaks I kind of do not know if I agree with Kayla!

Only because I agree with the part centralizing the

authorization authority for new entries and for the marketplace that

makes sense because want the PMO to be the main kind of distributor

of information and understanding.

I feel like we are moving this (inaudible) I do the know if

that means we do not want people to go through the sponsoring process

agencies are what the case is there.

I think Josh is point the agencies being the bottleneck and how

to get around that I feel like there has to be some sort of agency

mentorship program.

Or sponsorship collaboration program something like that for

first on agencies to go through the process even for agencies will

done this before may be are losing resources or whatever they do not

have enough resources to keep up with demand.

I feel like that kind of helps with the education kind of

getting some of the work off the PMO's back we all know that they are

super busy and if you are going through (inaudible) .

Just the process to be sort of the same across the board I think

one of the points adjustment was around the time it takes resources

the agency to get the work done.

When I was at my previous the agency (inaudible) history of

the process down to four guarantee weeks of resource time that was

specific to the federal point of contact.

We basically set it is going to take us for total weeks to

accept front two weeks to the end to get to this process. We put the

heavy emphasis on the work upfront.

Working with the CSP to say hey this is what you need to start

12

this process and if you are not at this minimum bar we are not going

to start the process yet.

I was kind of what Marcy was talking that is all. So if we can

get some minimum bar to say hey of XYZ ready we can start this

process and not only works on the CSP.

(Inaudible) were all talking the same thing speaking Fed ramp

101 here we can get things done. The CSP's can get what they need to

do done in the agencies can work on whatever they need to.

In the meantime and circle back to actually finish the job

there. Long story short if you like the education and putting the

work upfront will go a long way.

But I think there has to be some sort of incentive for these

agencies a to sponsor be to work with other agencies to get that

done. I am not sure if that is like a working group I know getting

workgroup set up.

Of the federal government is a long arduous process but I feel

like it would be worth the time and effort you have experience

agencies work together to help the smaller ones get through the

process.

>>LARRY HALE: (Inaudible) .

>>BRANKO BOKAN: (Inaudible) I'm a little for Christ I think we

been talking about barriers to entry for years now I think everyone

does agree no one questions that barriers to entry exists.

What surprised me today is that we really know very little or

have discussed very little with those actual barriers are I think one

of the issues with agency sponsorship.

Is one it's very clear but for the very long time we been

talking about the cost in terms of money resources and time. At

least I personally do not have any details are talking about

18 months to ATL.

Why does it take 18 months where what is that time I look like

is that the implementation it takes most of the time is it the ATO

being stuck somewhere behind the process on the fed ramp side?

(Inaudible) .

We need to better understand the timelines. We need to better

understand the cost we have been hearing numbers such as million

dollars to achieve a $2 million a year.

To maintain but where does that money go? Again we need some

type of break down so we can understand where the more significant

costs are and if there is something that we can do in terms of

13

recommendation to reduce that cost.

That cost money wise. Resources the same way. Do not know if

someone has any data to share that would be very helpful if we do not

have it we need to do something about it before we can make a

decision.

>>JOSH KRUEGER: Can respond to him without okay at least for

timelines with a go when you get up to schedule a three PO assessment

you get that done the of six to eight weeks.

For an SAR that is one sure of the point for three PO

assessment. The ghost your agency you have to do a star debrief with

them which usually takes a little but of time.

To get that scheduled based on their availability because again

everyone is tapped on resources right? It goes to them they review it

and then they start their full package review their ETO

(inaudible) .

Agencies that do a lot of them have done several for the VA

right there process is seven months long tissue in ETO. They are

doing everything needs to be done The process of just the process.

Others ordered energy for example the pretty fast they can take

like a month to do in ETO right it is completely dependent on the

agency and the individual workflows I cannot remember (inaudible) .

And then once it gets to ETO goes into the fed ramp queue for

authorization. You are in that queue which we have seen up to

26 weeks long previously so just from the sea the three PO

(inaudible) almost a year.

Depending on your agency. The VA is one of the top sponsor so

that is a lot of CSP sitting there in limbo there working through the

ATO process.

And then in the federal queue and then go to make remediation's

everything to get authorized once you meet the federal (inaudible)

do the review meeting.

That is all them sitting there burning consumption for the club

spend its them keeping people on staff to do continuous monitoring

running (inaudible) for their tools.

Updating documentation based on feedback from the three PO from

the agency from the PML. All these things play together for CSP is

especially small CSP's.

That just tab other resources across the board and if they're

having to do that ramp environment as opposed to a different

14

commercial environment.

Because they had to build a new environment to meet the

requirements then they their staff is split even further they have a

snowflake (inaudible) all the things kind of just stack up for the

CSP's.

They are sitting there paying for it all of their not able to

sell are not able to get customers live because they are not

authorized.

I do not have specific often anymore but I think until we are

able to send surveys out there kind of stuck not being able to get

that information.

Because people are not going to just put in the public comment

section saying hey we go with this three PO the charges this much in

(inaudible) .

>>BILL HUNT: Connecticut that I think we can the federal

government can indeed and should be sharing the costs associated with

these sorts of things marking side of the fence.

Released what we are spending on the vendors that we are using

for all going through the security process. The companies may not

want to.

But the federal government definitely should be able to share

that information because what we are spending our money on is public

data. Lease we have that side of it.

>>JOSH KRUEGER: And on my gosh are CSP's is more focused here we

do talk but agencies as well yeah and that priority that's at bronco

that was my response.

>>MICHELLE WHITE: Let's go to Michael head of team for a while I

believe Michael you also had some comments they put chat so we do

want to go over some of those comments to.

>>MICHAEL VACIRCA: Absolutely I did kind of just want to circle

around I did on off-line with some of the CSP's and brought together

on this party a problem statement and three actions they are CSP

related actions.

You may want to think about broadening them in this meeting. But

I want to try to focus us on what is the problem that we are trying

to hit on with this priority.

You want to take a look that I hope I have wrapped that well

enough to cover everything. We discussed. Out of the three actions

what we are really looking at least from the CSP side.

Is to say are there is their capability within fed ramp for us

to develop a tear compliance system or smaller low risk CSP use could

15

have a set of streamlined requirements to benefit the benefit there

being we could lower the cost (inaudible) .

The second item is really around can we establish a centralized

assistance program for small CSP's. Can we create centralized

technical (inaudible) .

And resources which we have discussed in previous meetings as

well and then is there potential for us to get an advisement to the

GSA administrator.

To potentially have maybe a staff member or an expert on staff

were some type of rotational program set up. Where large cloud

service providers and/or agencies can provide expertise to small

service providers I'm sorry to small cloud service providers.

When the third item is introducing the concept may be of

preauthorized compliance packages to also lower the barrier to

integrate around that concept we were really looking at can we

provide some sort of preauthorization (inaudible) .

Type of service that they are delivering a particular bucket

they would fall into the be able to use some of these preauthorized

packages or configurations to save time on their assessments.

And again reduce costs by inheriting these preapproved

templates. And being able to use them on their behalf. These were

three main categories.

From previous meetings again and also talking with CSP's were

kind of brainstorm and put together what would help level the playing

field for small CSP's.

As well as potentially lowering those barriers the entry

streamlining the process as recommendations that we can break to the

rest of the GSA administrator for the federal program itself.

I know there is a lot here I apologize for just getting this

all thrown at us (laughing).

Thoughts, questions I would love to debate these are the right

to the actions for you should be broadening them in some way adding

additional language maybe we could start with the problem statement

self at the top to see if we all agree with that.

>>LARRY HALE: We still have a couple of hands up but thank you

Mike both for the written input and your explanation of it. Really

greatly appreciated. Couple of hands have gone down Bill your hand

remains up.

16

>>BILL HUNT: Michael could you actually just elaborate on how

number one is not the existing tiered system today where we have low

moderate height and tailored?

It seems to be that that is a tear compliance system.

>>MICHAEL VACIRCA: Yes to it being a tear compliance system the

way that I was looking at this was (inaudible) a little bit more

around the CSP itself from like an infrastructure standpoint.

Some of at least the feedback we're getting together was a lot

of the infrastructure layer for some CSP's especially small CSP's is

being rated like a fed ramp eye level.

And then services with thin them are being applied at lower

moderate. There was concern that from even an infrastructure

perspective.

They would have to get their infrastructure at high first and

then be able to do some of these lower service levels. For their

individual services.

(Inaudible) the onus of how we have been pushing CSP

infrastructure in the past. The other thing were looking at here is

may be there's something here outside of the low moderate and high

that exist today there is a set of requirements we can put together.

For small businesses that might be a middle ground. Our between

different varying levels that brings together enough of the

requirements to create a small business that.

That might be something that there also talking about is a

perspective here. And again these are recommendations to the fed ramp

(inaudible) to really come up with.

(Inaudible) a blend of low medium and high again for that low

risk service low risk CSP which you would have to define in some way.

>>BILL HUNT: Picking at those I appreciate the clarification

first and foremost but I will say a couple of different things in

various (inaudible) .

I think fed ramp tailored covers a lot of that for what you're

recommending. Think we should be directing folks towards that as one

option.

The other thing I will say here and I will bring this back

around this as the federal government I am not comfortable with same

because your small business you should have a lower barrier

(inaudible) .

You present a greater risk to me is the federal government and

17

I know that is unfortunate I used to work for the small business

administration I want to see small this business (inaudible) I want

to see them in the space.

They do present a bigger risk to me then a large organization

primarily a lot of that cost for them is in that documentation. Want

to highlight your third bit here.

Because I think the large majority of small businesses that are

cloud businesses are sitting on top of a larger infrastructure

provider.

(Inaudible) as a result it is incumbent on companies like

yours really does the victory that I think to provide the hybrid

inherited control package for them to inherit from I would suggest

that this is not a fed ramp issue directly.

So much as fed ramp working with the big three providers to

make sure there is some sort of (inaudible) preauthorized

compliance package that covers that bottom layer that 60 percent of

controls that are responsible for.

Rather than saying they do not have to do it. I think there's

potentially wonderful opportunity there since that is most of the

controls for them.

If you didn't want to make sure you're doing that remaining

40 percent very very well at a high level of detail because if I do

not know that they know how to configure their account management all

of that all of the other controls that I do actually hear about.

Was of things and going to be spending my time looking at

generally speaking. As a federal agency taking them through the

federal process.

I do not want to give them a free pass played want to make sure

those controls they are responsible for are getting higher level of

attention to detail.

Agreed the principal but disagree on the approach.

>>LARRY HALE: Dan you have a hand up?

>>DANIEL PANE: I think one of the things was kind of mention was

through the controls that were inportant.

Or that people want to have and focus on I feel like that is one

of the things in the problem statement is kind of that minimum risk

threshold I do not know if I have the perfect solution for that.

18

I do not know anyone does. I'm curious if that is something

that the group wants to focus on or federal wants to focus on

something (inaudible)

1

>>DANIEL PANE: And said these are the 2025 or 50 that you cannot

fail XYZ on the other ones than we can have discussions around that

would be kind of interesting.

>>LARRY HALE: Jackie your hand is up next?

>>JACKIE SNOUFFER: Working on my controls here. Jackie Stauffer

(inaudible)–– I just wanted to echo what Bill said I do not think we

can have a lower standard for small business.

A lot of time they do not have the back and people and resources

necessarily to do a lot of incident response. Those types of things.

I just have got to echo that we have got to have the same

playing field requirements are there to reduce the federal

government's risk and hosting in the cloud.

We've got to figure out other ways to help the small businesses.

(Inaudible)–– inheritable packages this is something that we have

tried to do with the large vendors.

Is to create that inheritance model and I think it is really

important even if we can publish something that says if you host is

got to be an incentive right?

In the DoD there is an incentive to that because you can

inherit we only assess the controls that are not inherited from the

provider I think that is a critical thing.

I do not know if everybody is approaching that way. But I think

that would also help reduce the time requirements if we could get to

the point where when we look at a sass what does that mean need?

And what are the controls we expect from assassin

differentiating those from a provider that is got your infrastructure

in your (inaudible)––.

I think a lot of our small vendors are SAS providers. Looking

at the models that we use not reducing the requirements and

understanding who is responsible for those is really critical to

lowering that barrier to industry right to entry?

And providing a shared responsibility model or something that

they can start from I just think is really critical. You are all

talking about timelines.

Timelines is a funny thing just from an organization that does a

tremendous amount of authorization. So much of what we get is really

dependent on the quality of the packages.

I heard one person talking about we do a kickoff here we do a

kickoff there hopefully the multiagency construct is going to help.

2

But it is really important to do that upfront work and to understand

and I have got to foot stomp this particular issue.

Which is an organization going into a three PAO for assessment

before you meet with the client (inaudible)–– [video frozen].

Really my last point that I wanted to make starting with a low

does not have a lot to be quite honest we look at our defense

industrial base.

All of our contractors for using have to have a standard of

using said ramp (inaudible)–– so much of what we do starts at a Fed

ramp (inaudible)–– so we can protect our COI.

Even starting at the low you have gone through a lot of cycles

and a lot of work a lot of assessment just to get to a low does not

give you a big advantage so how do we make that barrier to entry

easier.

Through the inheritance models and some of those other types of

things. Just a few comments thank you.

>>LARRY HALE: Think you Jackie appreciate that very much. Before

we move on to Marcy and Joshua have their hands up I do want to just

invite committee members.

If you have edits to what you see on your screen you with them

in the chat proposed edits raise your hand and actually just state

the things the changes that you want to make and the producer will

live edit with you.

But please got about ten minutes left on this topic so I did

want to invite you to either submit it to chat raise your hand and

talk the producer through the edit that you want to make what that

will return to Marcy think you Marcy.

>>MARCI WOMACK: Again Marcy was shaman. Couple things I wanted

to kind of pay you back off of a couple of the committee members

regarding the minimum threshold of accessibility standardize baseline

kind of thing.

Mike there is the idea of the federal mandates there is that

table and it is very front and center in the readiness assessment

report.

That is like minimum baseline things that absolutely

100 percent have to be in place (inaudible)–– something to that

effect may be an expanded version of that.

Might get to the point that Daniel was making. Where as some of

those " high risk controls that term is not used as much anymore but

five or six years ago is to be used pretty heavily.

3

When we're going through the PMO review with DSPs for that Fed

ramp authorization is something to that effect might be helpful in

some standardization.

Secondly going back to Jackie's point about inheritance I think

that this the concept of apologize and (inaudible)––.

–– (inaudible)–– that is something I know that (inaudible)––

terms of how packages presented I do not know that there is a

mechanism by which to streamline that.

It may be helpful to do that in some kind of programmatic way

to be that is adopted was some of the Osco automated (inaudible)––.

>>LARRY HALE: Can we articulate that is a specific

recommendation?

>>MARCI WOMACK: I can do that do my best to drop in chatting

play with the wording from there.

>>LARRY HALE: Think you are like that appreciate thank you.

Michael?

>>MICHAEL VACIRCA: I did want to note that we do have an

alternative (inaudible)––.

I've gone ahead and shared that is been dropped in the text here

so let me know at this point of this one focuses a little bit more on

the automation.

The automation capability as opposed to crating a tailored

program for CSP's. Which we hopefully also reduce overhead for a

small CSP. Feel free to take a look over (inaudible)––.

More in line also I do have an alternative number three because

it sounds like number three is in line (inaudible)–– control

inheritance.

And to assure that right now for Darcy Marcy to drop in. It does

talk more specifically around inheritance as opposed (inaudible)––.

Marcy if you want to go ahead and drop that.

When it just adds a little bit more flavor around inheritance

itself. I think Jackie let me know that matches the wording that you

are looking for. Or at least the intention you're looking for.

I am out of alternative wording here. The rest should be up for

the committee to wordsmith.

>>LARRY HALE: Thanks I also want to think you will for the

research that you have done the independent research that you have

done that supports these recommendations. With that Josh your hand is

up next.

>>JOSH KRUEGER: Have we I mean just kind of on the DoD and on my

4

gosh– a lot of their systems are using GRC to pretty much DIY

(inaudible)–– I'm sure a lot of people you're familiar that.

Could that be used in any way in the Fed ramp side to help with

the processes in the inheritance. So if we have a package from the

Navy inherited from another system the inherited controls they cannot

even really look at.

(Inaudible)–– inherited across the board. Is there a tool like

that or could we leverage the mass (inaudible)–– on the federal

government side.

Just maybe that would help to ingest it could be the ingestion

point for the (inaudible)–– testing procedures and things like that

to expedite the review processes.

Probably (inaudible)–– more work for me later that was really

it. I do not know if that had been considered there is a reason it is

not being done and I am not aware that.

It seems to really streamline PTOs on the DoD site.

>>MICHAEL VACIRCA: Josh this is Mikey and we did go ahead and

put out a request for an RFP and I think (inaudible)–– building a GRC

tool on the Fed ramp side.

I am not the expert to speak on this I just wanted to bring that

up as that was something that was on the table and being worked by

the federal PMO.

Over the past I don't know six months from previous

recommendations.

>>JOSH KRUEGER: Okay thank you.

>>LARRY HALE: I think the next hand up his bill.

>>BILL HUNT: In response to what was just being said I'm

relatively certain most of the civilian agencies use one of two tools

to do this today.

All of their control management. Which it would be DOJ's see

Sam or Archer I guess would be the other one I a (inaudible)––

whatever I think those are probably the biggest one since the DOJ

actually owns one of those.

That might be something to think about but I do know that the

Fed ramp team we talked about this last season about them going

through.

And wanting to put together tool to be used for exactly this

that might be a hurry up and wait until that comes back around. My

other point that I wanted to ask about Tulare and friends as a point

of order here.

5

I assume the recommendations that were lining up here were going

to be going through and floating on as we did last season.

We are wordsmithing now but this is not the final final we are

talking about today am I correct in that?

>>LARRY HALE: You are correct. This is deliberation and

discussion and there will be time for actual deliberation on the

final wordings.

This is kind of live editing brainstorming and discussion which

I am loving. Because we are hearing a lot of good views I appreciated

Bill thank you. Branko your hand is up next.

>>BRANKO BOKAN: I wanted to remind my colleagues some of the

principles be on these (inaudible)––.

If you scroll up a little they need to be actionable, clear

cannot remember what else but also these recommendations are from

fizz cat to the GSA administrator.

Implementing something is not a clear actionable recommendation

what is it we recommend that GSA administrator does, who was supposed

implement.

Who is supposed to develop these frameworks that needs to be

clearly captured and that recommendation otherwise this will just go

nowhere. This is advice to all of them I am just commenting on the

first one.

>>BILL HUNT: No passive voice is basically the answer here.

>>LARRY HALE: Recognizing everything that we recommend to the

administrator somebody has to implement there will be resources, cost

that will take time.

We want to make these recommendations to improve the process.

That is our purpose for existing. Proving the process has to be the

objective thank you. After bronco I think the next hand up is

Jackie's.

>>JACKIE SNOUFFER: Hi thank you Jackie from (inaudible)–– what I

was going to focus on a really was the inheritance model in the GRC

tool there is a real need I think for all scow (inaudible)–– I will

confess that I am not an all scow expert so it may be there.

Is there a way in all scow that we can exchange an inheritance

package. This would start with bedroom talking about from an

infrastructure perspective.

What controls are typically inherited then having the CSP's to

be able to produce and their SSP or in something that says this is a

hybrid control this is fully inherited this is on the mission in

order to implement (inaudible)––.

6

Making sure we have the available fields in all scow so that

any GRC tool regardless of which one it is can actually bring that

into the GRC tool to make it available and also to be available to a

three PAO so (inaudible)––.

They know what controls to look at from a sass perspective I

just think this model the model probably belongs to Fed ramp to

produce.

We probably need to look at all scow to make sure we can

consume the inheritance model and then on the tool side we need to

look at what our assessors are using so that when they go out to look

(inaudible)––.

I think there is a whole timeline there that would actually

standardize as Marcy said I think this is something we do in the

Department of Defense but it is not broadly adopted.

We had to go down this path we really had to go down this path

because we recognize (inaudible)––.

I do believe there are actual items with various places from

Fed ramp (inaudible)–– that need to be done in this recommendations

space.

>>LARRY HALE: Think you Jackie. I do want to mention ten minutes

ago I said we had about ten minutes left on this topic because our

opening sessions sections I should save the agenda went so quickly.

In this discussion is excellent. We can give this discussion a

another 15 now 14 minutes.

Again understanding as Bill pointed out we are not waiting

today. We are wordsmithing. We are trying to come to a working

consensus.

On these recommendations without actually conducting a final

vote. Let's give another 1314 minutes to this discussion.

I am really appreciating all the perspectives and the thoughts

on these recommendations. There are no hands up right now I may have

just (inaudible)–– if nobody wants to talk.

Any as we are watching the live edits and mercy is responding

to what she is receiving in chat any additional thoughts, comments,

on what we have been discussing for the last 40 minutes or so?

>>MICHAEL VACIRCA: This is (inaudible)–– I edited in language to

cover the GSA administrator (inaudible)––.

Organizations part of the organization. Does this cover what you

7

were looking for specifically?

>>BRANKO BOKAN: Yes I think (inaudible)–– this is more along the

lines of what our recommendation should look like.

>>MICHAEL VACIRCA: Awesome.

>>LARRY HALE: Knowing as the said we are making our

recommendations to the GSA administrator but ultimately as you point

out the GSA administrator is not going to do these things.

He or she, she right now, is going to recommend that somewhere

in the federal process that these things happen.

Recognizing also the limited resources of the Fed ramp program.

Let's make our recommendations actionable. And impactful if we can

please.

Take a few minutes, read what is on your screen now because we

have tweaked them as we talked. Read what is on your screen now.

After a couple of minutes we will if we do not get any hands up

any concerns about what is here we will roll into our break and move

on to our next agenda item after the break.

>>MATTHEW SCHOLL: Hey Larry (inaudible)–– implement the

streamlined compliance framework. But then all of the actions and

activities are around automation of current compliance framework.

Is this really what we are doing (inaudible)–– last sentence of

that paragraph which is reducing time.

Two authorization rather than a streamlined compliance

framework? I keep circling back (inaudible)–– redressing symptoms or

causes.

And also keep mulling on that one I think we may have drifted

away from the streamlined compliance framework to actions that reduce

timeline two authorization.

>>LARRY HALE: Are you saying that we should change this to

streamline the existing compliance framework?

>>MATTHEW SCHOLL:

>>MARCI WOMACK: I think implement is perhaps not (inaudible)––

the correct verb there.

>>MATTHEW SCHOLL: I think the goal we are working for is to

reduce the time and on my gosh I.

>>LARRY HALE: Yeah cost and varies will have to see how that

plays out.

>>MATTHEW SCHOLL: (Inaudible)–– [video frozen].

>>MARCI WOMACK: It is very complex and there is a lot that is

very inter-dependent on each other.

8

I think it is difficult to not kind of go back to some of the

items we have talked about previously I just want to make sure

there's an opportunity did the conflict in the previous

recommendation memo.

>>LARRY HALE: Great point Marcy. And I see Bill reacting with a

thumbs up on that.

>>MARCI WOMACK: Perfect some of it just sounds early similar

(inaudible)–– I am also repetitive so.

>>LARRY HALE: It is only to me because I was not here last year

just kidding like Pete said at the last one he spent time listening

to every Fisk CAC meeting I too have read every word that the fist

CAC has published.

It really eerily similar is always fun. All right is anyone in

need of a bricked we want to discuss these first three further?

Knowing that we will have a chance to deliberate them on vote on

them at a future meeting are we comfortable with what we have written

right now for now?

Mike?

>>MICHAEL VACIRCA: I would love to give Marcy your feedback

there is enough focus (inaudible)–– that was one of the top lines

from the priority itself.

>>MARCI WOMACK: Agree I am more of a digesting kind of process

I'm a processor. Going through the slide is always a challenge for me

personally.

I think yes I want to make sure that I can go through this and

collaborate with the three PO community as well just make sure that

we have captured it.

I think number two is important because that often has some real

direct (inaudible)––.

Also number three is very assessment impacting as well as well

as how the agency adjust the information. Noted.

I would like to kind of take that as an action following the

meeting.

>>LARRY HALE: Marcy I appreciate that and actually all the

committee members and members of the public who are observing today's

meeting we would welcome your comments.

We want the committee to do to continue to do their deliberation

of research. We want public comments as well.

Thank you all for that. We are I think at a point where we can

take a break. Michelle?

>>MICHELLE WHITE: Great let's go ahead and take a ten-minute

9

break actually 11-minute break and we can be back at 120.

>>LARRY HALE: Thank you Michelle think everybody. [Recording in

progress].

>>MICHELLE WHITE: All right welcome back think you guys for all

of your participation today we have had a great conversation so far.

Who like to go ahead and move to our final topic for the agenda.

Larry would you like to kick us off summarizing our next steps

from this meeting and recapping any closing remarks you may have.

>>LARRY HALE: Yes. Let's see let me turn my video on. Either way

without turning my video on thank you all for the great discussion

(inaudible)–– of our recommendations of our priorities.

Let's see let me get in the right place we basically just want

to continue the same deliberation. Around our second priority for

about the next 45 minutes or so.

Looking at the second priority (inaudible)–– the authorization

process for CSS. (Inaudible)––. Both labor and financial with a

focus on small businesses.

E.g. ensure minimum risk threshold (inaudible)–– or sponsoring

agencies and note that we have received we have received some

committee notes that are at the bottom of the screen now. On this.

This again we want to create a problem statement.

And actionable specific recommendations for this one just like

we did on the first priority in the first chunk of this meeting. Who

would like to kick us off with an initial thoughts on the problem

statement or recommendations?

I invite you all to take a minute read Kayla's notes at the

bottom of the screen and let's take it from there I hope our

discussion on this priority is as robust as the first one.

>>BRANKO BOKAN: Could we see the statement again please. Okay

radio some hands up we will start with Jackie and then Bill Jackie.

>>JOSH KRUEGER:

>>JOSH KRUEGER:

>>JACKIE SNOUFFER: (Inaudible)–– just an idea generator. From

the three PAO our team actually does a quick risk review and then I

actually issue and ITT that allows the sponsoring organization to go

through and start their buildout start testing with the

infrastructure.

10

They can pass (inaudible)–– but it does allow them to move

forward so they can begin to test and to build. They can purchase.

It has accelerated in the not allows us time to finish the

actual mechanics of issuing the provisional authorization in the

department. And so it is we can go forward in the department with

EPA.

We do not have to wait until it goes on to the marketplace. We

go forward (inaudible)–– going to the marketplace allows the federal

side of the house to leverage our authorization.

I do not know what type of reciprocity you have if you're in the

Department of the Interior you are let's say in the Park service and

the authorized the cloud could other interior agencies actually

leverage that correct?

Before goes to the marketplace? What is the reasoning behind

going to the Fed ramp marketplace? It is an interesting construct but

we do allow testing at that I ETT phase we have found that actually

helps both the user.

The mission owner, as well as the cloud service provider to

actually be able to start working toward the final authorization that

opens up the floodgates for the rest of the department.

It is a testing at least it is a testing in a process is

working can we get on with our Cards and all those kinds of things.

Is just a suggestion and it could probably be broadened out and

more generalized I just offer that as a concept for consideration in

terms of a recommendation. As we go forward.

>>LARRY HALE: Thank you Jackie Bill?

>>BILL HUNT: (Inaudible)–– lightweight ITO, we call ours and

authority to guess. Everybody has some version of that thing.

I do not think it is beyond reason for the Fed ramp program to

be able to issue something like that and I do not think it is

necessarily bad recommendation (inaudible)––.

Please do not take this to production until the work is done

because you should not be issuing an ATO against the provisional ATO.

Something like that I think we would really clarify.

Strongly agree that if one agency is doing it and that should

be good enough for all agencies of it has the Fed ramp seal of

approval somewhere on their for some set of controls that can be

generally reapplied universal.

11

I think that is generally good. I also note that Kayla brought

back the inheritance a point here that we brought from the previous

(inaudible)––.

Blessing I wanted to mention was the third point here with

regard to the exception process. Am sure everyone is sick of me

talking about this. But I'm going to talk about it again.

This committee proposed to OMD that there needs to be an

expanded process that match the original exception process because

this is disadvantageous to small business as well as to large

businesses.

That have cutting-edge solutions that need to get in the hands

of the federal government faster. OMB is: And said those have to be

categorical. I do not think categorical is sufficient.

I foot stomp Kayla's getting at here which is some offers will

never be able to afford to go through the Fed ramp authorization

process.

Because it is more expensive than going through a lighter weight

ATO process that is just the facts folks. We need to be

understanding.

That's I would say if this is a memo to the GSA administrator

she is in a unique position to ask OMB to do the thing that they

ignored us when this committee asked for instead. I would ask that we

ask again.

>>LARRY HALE: Thank you Bill Ronco your next.

>>BRANKO BOKAN: I would follow-up that I was just looking for

the list of participants but was not here today and I think he

proposed this in one of the early this Meetings.

And I think it goes hand-in-hand with this recommendation not

only the exception to process that a tasking I do not know if that is

OMB Fed ramp (inaudible)––.

To come up with an authoritative guidance on the thresholds for

ATO authorization if I remember correctly he was talking about

instances where ATO is not necessary.

But because the guidance does not exist agencies tend to over

authorize even instances of services that do not necessarily need to

go through (inaudible)––

I think it goes hand-in-hand with exception/thresholds.

>>BILL HUNT: I still do not know if we ever got that written

down.

12

>>MICHAEL VACIRCA: Bill I also wanted to add on a clear

definition clear definition (inaudible)–– would be nice.

Highlighted right now is a problem statement that I wrote a

seven was talking I am trying to keep a high level on this one so

please feel free to throw stones at it.

I do not know if it hits everything that was in the priority or

not I think it does I just developed it on the fly.

>>LARRY HALE: Go had.

>>MARCI WOMACK: Apologies this is Marcy just wanted asked for

clarification of my understanding of the priority this is

(inaudible)––.

Expediting the authorization process of shortening the time when

correct? I guess we also say other cost reduction okay primary focus

would be timeline authorization sub focus would be cost reductions as

well.

Which feeds into that.

>>LARRY HALE: Marcy great question is going to ask where you say

inconsistent requirements do you mean that the requirements are

inconsistent, or the way that that they are enforced is inconsistent.

>>MICHAEL VACIRCA: Is probably the latter so it's application of

and that would probably clarify that right inconsistent application

of requirements or validation potentially as well might be another

good word in there.

>>LARRY HALE: Thank you.

>>MICHAEL VACIRCA: The point I am driving on there is we see a

cost (inaudible)–– as well as authorizing agencies different

interpretations even in costs across different authorizing officials.

Or TR's like we see different levels of what is acceptable or

not and where we are. That leads to non-standardization and also also

a little bit of a shell game by CSP so they try to find places they

can have an easier authorization process.

>>LARRY HALE: Yeah it comes back to what was discussed in the

previous discussion for the break about what are those things that

are boldfaced.

That are absolutely pass fail? And what are those things that

can be grouped together as some combination of these must be met to

meet the threshold.

There was a comment in the first discussion around transparency

that said we need to clarify what is absolute must have pass fail.

And then what is that next here of requirements that are

13

aggregated? I hope I am not misinterpreting that or misapplying that?

>>LARRY HALE:

>>MICHELLE WHITE: Jackie go had.

>>JACKIE SNOUFFER: I'm going to drop this and chat (inaudible)––

would be for Fed ramp to implement a quick package look and issue an

interim use on the marketplace for CSL.

This would allow agencies to go ahead and use a CSO at their own

risk will Fed ramp continues the full evaluation.

I think one of the things that would be interesting to learn

from Fed ramp is how many packages and CSO's do they actually not put

on the marketplace?

Come into them. I think there are challenges with some of you

can always work through but I think that would allow faster use of

the CSO for them to recover their costs.

That is one of the things I've been hammering I know we have we

connect to our (inaudible)–– it takes a long time to get connected

are provisional authorization process we been able to speed up the

connection is a little more difficult.

Streamlining these processes are just so critical and I foot

stomp this with everybody that touches this that this is really

expensive for our cloud service providers and we have got to find

every means possible to manage our risks.

And help the CSO's manage their financial risks so we can use

their products. That really is getting to a market point where it can

be used.

I think that is just really a critical thing to keep in mind

that if you can do a quick look can go ahead and let people use it

while you're working through some of the details that Fed ramp needs.

>>MICHAEL VACIRCA: Is had a quick question on that would you be

looking at that as potentially varying levels of authorization based

on varying sensitivity of this EO I data?

Are you looking at that as varying control application

compliance levels for varying ATO? If that does not make any sense I

can give an example.

>>JACKIE SNOUFFER: Having trouble coming off mute sorry I look

about it somebody talks about one of those critical controls is in

authorizing officials the ones that I really look at our auditing and

authentication.

Other AO's have various families that they need to look at but I

would look at this as not varying levels but a quick look to say here

are my top 20 or 30 controls as opposed to all 400.

14

And this looks like a tight package it is good there is an

acceptable risk in the department we have a concept of red controls

those are perimeter controls and we have yellow so we picked out the

subset.

Before we will allow a system to connect this 25 or 30

controls. And so they can start their testing process and all that

type of thing.

That is for regular systems but that is what I'm thinking is

just a smaller subset of controls that are deemed really necessary to

be able to protect COI in a moderate package.

And let it go forward you could apply that to say were not

going to process PII. And exclude that way because sadly the COI

registry is way too many items on it.

The PI PHI is one that is easy to pull out and say okay that

when you cannot do it is for anything but PI I PHI. Those are just my

thoughts.

>>MICHAEL VACIRCA: Got it going to recommend an action asking

projecting benefits based on that thing aligns with what you're

saying.

Because I have been drafting something similar some going to

send it over to Darcy and see if this answers are aligns with what

you are saying Jackie. It will show up in the document shortly.

>>LARRY HALE: Thank you Jackie Marcy do you have your hand up

you had it up to you want to speak?

>>MARCI WOMACK: I lost my train of thought I will raise my hand

if I come back to it.

>>LARRY HALE: Gotcha thanks so much. I am loving the thread that

is going on here.

Jackie something you shared that is practicing the department I

put in the note here that it could be a best practice that we could

with red and yellow controls.

That mainly what we're talking about here about the boldface

must haves and then the idea of a quick look and a package check and

then a certain level of authorization to move forward.

It is something we should definitely be considering Marcy your

hand is up.

>>MARCI WOMACK: I am back think you (inaudible)–– for a few

reasons I also like to say some of this exists in some capacity

already.

There is never much to the chagrin of the DoD Fed ramp of the

15

equivalency my mother is never if ever a Fed ramp package that has 0

findings are 0 risk unit there is the idea are federal authorizations

being granted.

Week in and week out that are two systems with existing risk.

There is a risk-based decision being made based on what risk is

presented to say hey we are good with this provided that you close it

within (inaudible)––.

There is some sort of structure for this already. If we could

do it programmatically was some of the automation that is in the

pipeline.

I think there is a huge benefit that plays into anything

everything that Jackie and Mike have been talking about here.

I one more question for bronco as it pertains to like the work

they will have done with the Fed ramp program is there to think there

is existing data in terms of maybe categorizing controls into higher

levels of risk?

>>BRANKO BOKAN: Yes I was just looking for yesterday

(inaudible)–– direct modeling the Fed ramp about two or three years

ago.

A lot of that those results would need to be updated but the

data exists we just need to find it I would allow us to prioritize

853 controls based on the threat that we have observed in the wild.

Not theoretical but very exact privatization based on actual

threat actions in TTP's that industry has observed in the wild. And

that allows us to not only prioritize controls.

Based on the coverage against those threats but also based on

frequency of those threats. That would allow us to come up with a

list of top 1520 whatever it is controls really matter.

(Inaudible)––.

>>MARCI WOMACK: Think I love that I think that would be a great

thing to integrate into this discussion in terms of it exists may

need to be updated but that's okay in terms of having a starting

point to tying all of this together.

>>LARRY HALE: Absolutely think you Marcy and bronco's we have to

remember that we are Fed ramp stands for respites risk management we

cannot avoid all risk.

But understanding the equation of risk includes the probability

of happening is a huge part of this so that will be really cool and

very helpful thank you.

Mike?

>>MICHAEL VACIRCA: Just curious on a risk-based question would

16

be beneficial for us to recommend to the GSA administrator to meet

with NIST.

Or the other agencies that would be alert able to provide that

kind of standardization on controls and what controls belong to which

category or family categories.

I think that might be the organization but I just do not know

if someone is a little smarter than me.

>>LARRY HALE: Matt is our NIST rep met had to drop for a few

minutes I don't not know if he is back yet and (inaudible)–– did you

want to comment?

>>MICHAEL VACIRCA: Or other agencies to participate in the

development of that since we are looking at creating basically a

standard.

So rather than federal interesting there shall be the standard

to set something we should be partnering or working through other

organizations within the US government definitely whenever it comes

to any type of authoritative definition.

>>BRANKO BOKAN: (Inaudible)–– for cybersecurity as well as nest

they need to be consulted so this would ever be developed in a vacuum

I non-policing bodies.

>>MICHAEL VACIRCA: Okay perfect Emily asking not because I'm

trying to draft something up on the baseline and I want to make sure

that we have it correct.

>>LARRY HALE: Yes thank you Mike in terms of obviously nest

manages the standards and Sessa helps to set the prioritization I

think bronco characterize that I characterize that fairly accurately

thank you Bill.

>>BILL HUNT: What I just said oh of CIO office of OMB.

>>LARRY HALE: Office of the CIO at Office of Management and

Budget.

>>MARCI WOMACK: They have most of the (inaudible)–– just in the

grand hierarchy of things.

>>MICHAEL VACIRCA: Got it sounds good I think I have it correct.

>>LARRY HALE: Yes bill. It is in government terms it is fairly

streamlined. Course of my personal comment not representing the

opinions of my agency.

>>MICHAEL VACIRCA: (Laughing). I through some language together

and I'm sharing it with Marcy right now around what we just discussed

let me know if I captured that properly especially on the ask part.

>>LARRY HALE: Marcy your hand is up.

>>MARCI WOMACK: It is think you Marcy was shown when I was

rereading a priority statement and we have been focused on

authorization and largely the initial assessment process one thing

that we have not spent much time on.

Is the readiness assessment. The RAR process in the federal

program I will say it has changed significantly and evolved over time

17

since it was rolled out and I think 2017.

– kind of the idea initially was was the readiness [no audio]

cloud service offerings ability let me know if you all can't hear me

in getting the unstable alert on my zoom.

Around the ability for organization to actually be successful or

offering to be successful and it goes to the initial (inaudible)––. I

think that some of the steering that we talk about the process might

want to be considered.

Not because think that was some of the house of evolved to be

much more I would say cumbersome and detail oriented but I just

wanted to throw it out there because I think it is impactful.

And might solve some of these things that we have identified

maybe not necessarily authority to test but may serve a role in that

tearing that we have discussed really much experience but it is

something that still does exist within the program and provide some

of that capability.

>>LARRY HALE: Think you Marcy we only lost you for a second or

two. We definitely caught most of everything you said.

>>MARCI WOMACK: Perfect, thank you.

>>LARRY HALE: Additional comments, thoughts?

>>MARCI WOMACK: If there are none I can think about it as I do

are secondary review and add in some commentary where I think it may

be appropriate for later discussion.

>>LARRY HALE: That would be great Marcy greatly appreciated. I

really the individual research that committee members are doing that

is bringing to these suggestions and these proposals is extraordinary

helpful and I appreciate it. I have one it's in.

>>MICHAEL VACIRCA: Have one in a new thread (inaudible)–– we

explored for small service providers there is an ability for the US

government to do some kind of financial support incentive program for

us to we have in on my–.

This JustGrants in general some sort of cost sharing models for

them is that something we've ever thought about her explored? An kind

of pitching out there in general not to directly.

>>BILL HUNT: This is Bill again I feel like we talked about this

a couple times about potential opportunities to get some work done

through the SBA and a loan program for small businesses to target.

Specifically around cybersecurity enhancements and things like

that. I do not know if there is an existing fund there I do not

believe there is a dedicated one but there are general grants

available there.

Definitely something that potentially could be taken up by the

legislative side of things particular for those of you all were

18

allowed to lobby.

That would be something to think about.

>>MICHAEL VACIRCA: Gotcha didn't have an appetite may be under

this priority since it is one of the we focused a lot on the time for

authorization.

There is also the reduction of cost I believe in the priority

language but this be something other cost reductions this be

something that we would want to may be potentially draft up as a

recommendation?

>>BILL HUNT: Did we recommend this last year is my only thing I

thought we specifically said something about that but it could be

wrong. (Inaudible)––.

>>MICHAEL VACIRCA: Let me go double check on that one.

>>MARCI WOMACK: Again I am a massive Department of small

business loans.

>>BILL HUNT: Disadvantage small businesses personally.

Particularly to be able to compete in this arena. I think that is an

excellent idea I would like to see more attention to it.

If at all possible. It looks like I am being live fact checked I

thought we said there is not going to be in effect checking.

>>MICHAEL VACIRCA: (Laughing).

>>LARRY HALE: Oh dear Mike your hand is up?

>>MICHAEL VACIRCA: Were you able to find it or not in that

search if not we should I can draft up some language maybe if we want

to consider it.

>>BILL HUNT: (Inaudible)––.

>>MICHAEL VACIRCA: Sorry did not catch that on my and it came up

a little garbled.

>>BILL HUNT: I was just saying I'm happy to collaborate with you

on that if it is at all helpful.

>>MICHAEL VACIRCA: Cool I will throw together something quick

and we can throw it into the notes and then review it off-line and

come back next session.

>>BILL HUNT: Perfect.

>>LARRY HALE: Thank you.

>>MICHAEL VACIRCA: No problem (inaudible)––.

>>LARRY HALE: Does anyone need to scroll to a different part of

the screen additional thoughts, input?

Right now the top of the screen there is the priority we are

discussing that is our draft problem statement and then we have a

nice (inaudible)–– obviously we need to tweak them and make sure.

Like we did with the earlier discussion that we make it clear

who and what this is a great start. Want to give everyone time to

follow what is going on on the screen.

19

Because the seventh draft recommendation has been added with

some parts so again take a look at that, jump in, raise your hand

with questions or comments.

If you want to add additional subparts and at the ones that you

see or add another one. Go?

>>BRANKO BOKAN: Once again explore and establish but who? Who is

that recommendation for we need to be very specific in terms of our

expectations.

>>MICHAEL VACIRCA: That's a copy pasting hold on Marcy is

cleaning it up right now.

>>LARRY HALE: And Joshua (inaudible)––.

>>JOSHUA COHEN: Sorry I was late today (inaudible)–– I just had

a question on this is going to suggest perhaps the SP a as well

(inaudible)––.

Is also interested is that something where the agency in a

similar way that in agency sponsors (inaudible)–– to ensure that we

are now Mike–– someone have the right interest and willingness to

work with that be something that we would want to lead into that.

For that financial in order (inaudible)–– a small company

decides (inaudible)–– sorry if that was something as mentioned

earlier.

>>LARRY HALE: I do not think it was mentioned earlier I

appreciate you bringing it up thoughts from the committee? I did hear

you say not just GSA's (inaudible)–– also the S PA MI is

characterizing that?

>>JOSHUA COHEN: No.

>>BILL HUNT: (Inaudible)––.

>>LARRY HALE: Thank you Bill.

>>NAUMAN ANSARI: This is (inaudible)–– I was not able to raise

my hand there just a clarification on the loans the authority to

establish a loan program.

Closest to the appropriations so that would be something we

would have to work through the appropriators and is not something the

SPA could stand up by its own.

>>BILL HUNT: Sorry doubling down on that the threat is

mentioning earlier there is existing authorities (inaudible)–– four

loans for small businesses but not specific to this topic.

>>LARRY HALE: Yes so if thank you again if we are making

recommendations to the GSA administrator some of these

recommendations we must recognize some of them may require

legislation etc.

Understanding what the timeline is and what we are asking for

that does not restrict us from making the recommendations.

If we think that is what is going to help address his

20

priorities. Bronco your hand is still up.

>>BRANKO BOKAN: My apologies.

>>LARRY HALE: Not at all. Again I really appreciate the robust

discussion, the screen fall of language and all the thought that this

reflects the work that you've done between meetings.

In the equities you are all bring to the table. I do not want

to cut it short but I do want to express my gratitude and

appreciation for the committee members and the thought that you are

putting into this.

Understanding as we clarified earlier that this is not the

final part we are not voting on these today we are not finalizing

them this is our initial proposal.

And we understand that we are going to I think it was Marcy that

said I need time to think digest and process and we do so between

this meeting in the next one we will have time to review these, think

about them, engaged with our stakeholder communities.

As individual research and then come back to the committee for

the deliberative process. So, if there are no more thoughts if there

is no more thought discussion on priority to,.

We can also go back to priority one if the committee wants to.

Use the time you had a couple of folks that were not able to be here

for the first part of the meeting. One more look at that we may end

up wrapping up a little early today.

I want to use your time and want to respect your time and I

want to use it well because I think we have had a very productive

meeting to this point.

So on the screen we've gone back to priority one in the problem

statement that we we worked up in the first part of the meeting. Just

to give everybody a chance to look at that. Think about it.

And again we understand that we are not voting on these today.

>>BRANKO BOKAN: Mary I am assuming you are not looking at your's

greener couple of hands raised. I figured that you also looked away

thing.

>>LARRY HALE: Thank you I appreciate that bronco first and Mike.

>>BRANKO BOKAN: Thinking back about my previous comment about

not really having enough data about the timelines costs in terms of

both resources money and time I guess.

How do we know that these recommendations are really properly

prioritized that they are hitting the most significant issues and the

barriers to entry? Again I really want to raise this question with

all of my colleagues do we still need to do addition to need

21

additional data? Or does someone need to do additional research.

We feel confident that what we have here is recommendations

will address what we believe to be the burden to enter your barriers

to entry?

I just want to make sure we are not distracted and are not

moving in the completely wrong direction just because he did not have

the data to address the original problem bronco that is exactly why

put my.

>>MICHAEL VACIRCA: (Inaudible)–– we did talk in the past around

I will this mentioning is one by one we talked about preassessment

tools for faster authorization and automation on that which I think

we have addressed in priority one.

Talked about a rep or process reciprocity framework in the past.

We do have a marketplace I'm crossing that one out.

We talked about provisional ATS which I think we actually

included in this one on the first half. Continuous monitoring and

recor.ding there is another area that was a major concern around

cost.

Especially in the agency side of the house and I think Jackie

was a big proponent of anything we could do to lower that to reduce

that cost.

And then there's some other smaller things to talk about the

past could not click public-private partnership open source

compliance.

Or open compliance and we also talked about low hanging fruit

was regular M training and workshops and then also documentation

single source of documentation.

Those were some of the major categories that we have talked

about before. I can repeat those for anybody of any of those trigger

you (laughing).

>>BRANKO BOKAN: Given everyone else's limited resources we

should probably consider in our future discussions prioritization of

these recommendations and also reducing the number of

recommendations. To a meaningful number.

With the biggest possible impact.

>>LARRY HALE: Excellent suggestion my can still up?

>>MICHAEL VACIRCA: Sorry that is just taking it down.

>>LARRY HALE: I did not want to not call on you. All right I

think we have got a lot of material here today to take back, think

about, deliberate on.

22

And come back to the next meeting with additional comments

recommendations we are not going to take a break I do not think so.

With that let me just turn over to Michelle and do I roll right

into closing remarks.

>>MICHELLE WHITE: If you would like we are at the final topic of

the agenda today so if you would like to just kick us off summarizing

our next steps from this meeting and recapping any closing remarks.

>>LARRY HALE: All right will listen again I am just so

appreciative of your active participation in today's meeting.

I think we have made really great strides in our initial

drafting of our report to the administered on the first two

priorities.

Before closing today would like to ask you all the committee if

there are any gaps that would require further information or

clarification during our next meeting.

In order to start finalizing the recommendations for these two

priorities and also other additional specific speakers.

That we would like to hear from? I'm kicking that back out to

you any gaps or clarification on what we did today, and any specific

speakers that we would like to hear from potentially in the next

meeting

Might? We've got Mike Bill and Jackie in that order.

>>MICHAEL VACIRCA: On the speakers I think having (inaudible)––

and give a sense of how the first 3060 days are going for him as the

director. With things he is prioritizing where he is focusing now

that he is starting to get into the role.

>>LARRY HALE: Thank you Mike. I think Pete is listening to this

live, we will take that down as a request a speaker request.

Bill?

>>BILL HUNT: I am always down to hang out with Pete that sounds

like fun to me I would also recommend I do not know if we can share

whatever draft version we have coming out of this meeting for public

feedback again.

I feel like the last meeting we got a whole lot of really good

comments but I think this is another good opportunity to ping the

community and see if you're getting it right or not.

Or if there are other ideas that we are not considered I know

we've all read through (inaudible)––.

The submitted comments very closely and seen a bunch of things

in their just whether or not folks have other specific ideas that we

23

do not cover today.

And that could improve things for again particularly my

attention to small businesses with the overall program I think this

would be good opportunity to provide that feedback.

On these specific topics. Just put a call out on LinkedIn and

other social medias for that always happy to repost.

>>LARRY HALE: Bill absolutely great suggestion I can tell you I

had folks come back to me after I posted posted that request on

LinkedIn.

Encouraging public comment and it even resulted in a mention one

in media mention that the fizz CAC is looking for public comment and

I was thrilled about that.

Encourage all of you to use your social media channels to draw

attention to the work we have done today.

And invite public comment and for the members of the public or

participating in today's meeting, please submit comments on our form.

>>BILL HUNT: I will say the media mention is a good point

(inaudible)–– that would probably be helpful as well putting that out

there.

>>LARRY HALE: Thank you Jackie?

>>JACKIE SNOUFFER: Two things this very well may have been

discussed at the last meeting that I missed and I do apologize for

that.

But where I would like to hear what GSA took from our memo and

what has been implemented by Fed RAM or the other people that were

callouts in last year's recommendations.

The other one is where are we in the transition and with the

OMB memo? I have a perspective that may be different from others.

I would really like to hear and I am concerned from our cloud

providers and for my three PAO's do they believe (inaudible)––.

Is a good, bad, I think that may inform some of the things that

we may recommend to the GSA administrator where we might end up with

gaps in the implementation of the OMB memo. Over.

>>LARRY HALE: Thank you Jackie I think your comment has

generated a couple more hands so we will go to Matt next and then

Marcy.

>>MATTHEW SCHOLL: Thank you Larry actually thinking about

something a little different. If you cover this I apologize I had to

step out for a little bit from a call from my boss. As far as next

steps we are on CR until December 20th.

24

As a Fed I am often very concerned about asking agencies to do

something without having them properly resourced to make change let

alone continue with current operations.

May be this is a Pete talk but how has CR potentially affected

resourcing and the potential impacts to achieving the goals that the

program is looking for.

And then how can we as a board advocate for the program so they

are properly resourced? To achieve those goals?

>>LARRY HALE: Thank you Matt. Appreciate that. Marcy has

captured everything perfectly.

I said Darcy I said Marcy when I wanted to say Darcy Marcy

Europe next.

>>MARCI WOMACK: No problem I been called much worse. My question

relates off of Jackie's comment I know there are so many things that

I think would be helpful.

Or that are relevant to our two priorities and they already be

on the roadmap as a result of the OMB memo or just on the overall

program modernization.

I'm curious had a thought earlier and withheld it I guess I'm

curious is there any guidance that you have for the committee members

have and when it may be appropriate to kind of include that in our

commentary and recommendations here as it is relevant.

I do not want to duplicate either but I want to make sure if

there's things like the program authorization as an additional way to

access Fed RAM.

I think that is really key so I just want some guidance on when

it may be appropriate to include that type of information may already

be covered.

>>LARRY HALE: (Inaudible)–– we all know when the memo came out

and we have all I think particularly those of us who are government

employees understand the time it takes to react to an OMB memo.

Time it takes to implement a program implement priorities etc.

These things do not happen overnight. However getting an update on

the timeline I think is a reasonable request.

That way as you pointed out as we work on these priorities as we

work on our recommendations we can understand how they fit and that

we are not recommending something that is already being done. So

thank you for that. Any additional hands?

I am seeing none. Michelle? Let me turn the meeting over to

you.

25

>>MICHELLE WHITE: Are great thanks Larry. I want to thank

everybody again for joining us today we really appreciated your

feedback and participation.

With that I will go ahead and adjourn our meeting we have taken

notes and will be in touch with our next work meeting date thank you

all.