I'm Matthew Donkin from AWS and I'm joined by Stephanie.

Sure that would be good as well going to present some other lessons learned for AWS from our first OSCAL submission of an SSP to FedRAMP and some of the things to be, kind of at a higher level. What we have gone through to get it done and some of the lessons learned to share with others and with that, I'm just going to dive right in.

The first thing is the format
challenges. So one of the issues that we've had was aligning some of our documentation and the various
documentation to the OSCAL format for specifically FedRAMP with how our SSPs are written is very differently and we have various dependencies which cause some issues Getting those into the proper format and I'll go over that a little bit more on the next slide And then, with our POA&M ... we have some extra information within our POA&M as well that will be causing a little bit of issue in the future that we... we're kind of going to be working through it right now But really, what it is right now, is taking that that documentation and getting into that
digitized format which we knew was not going to be

a very very easy lift. We knew there was going to be issues setting out for this.

So a lot of this was kind of like we know what was going to happen and we are working through various plans right now to kind of get everything aligned for that

machine relatable OSCAL format and the SSP challenges. So we have ... we have our commercial boundary and our gov cloud boundary which each have a main SSP and three appendices for each for the IaaS, PaaS and SaaS offerings and this cause them trouble when we put it into the OSCAL format for FedRAMP specifically. So
we had to have a solution. Then our ...
temporary solution right now is just to

32
00:02:03,920 --> 00:02:08,640
have a separate OSCAL formatted SSP for
each of those

33
00:02:08,640 --> 00:02:13,520
offerings. Right so you have one for IaaS PaaS and SaaS for our
commercial

34
00:02:13,520 --> 00:02:17,440
offerings and one for IaaS PaaS and SaaS
for our gov cloud offerings. As long as

35
00:02:17,440 --> 00:02:22,480
we got independence for all other appendices
for IL5. So it's seven documents

36
00:02:22,480 --> 00:02:26,560
right now for all of our SSPs and their
dependencies which is

37
00:02:26,560 --> 00:02:29,840
not
perfect but

38
00:02:29,840 --> 00:02:33,440
it's what we have for right now and
we're gonna be working towards that

39
00:02:33,440 --> 00:02:38,560
single two SSPs: right, one for commercial
one for gov cloud is what we want our end

40
00:02:38,560 --> 00:02:41,519
game to be in the future.

41
00:02:43,120 --> 00:02:46,319
And some of the implementation
challenges. There's multiple work streams

that go into providing this information and not

all work streams were really on board at first for OSCAL even um

within our organization so we had to really sell it and show the benefits

right and that is something that was actually fairly easy to do once you got into the
to what you could do with this

particular format um and so once you get people on board you get everybody moving

in the same direction, it created issues with managing that workflow. So instead

of just managing for our one team we have to now manage across multiple teams.

And there's some erroneous information that

it was asked.
One of the..one of the template issues was: "How many users are on the cloud at one time". As you know we're a very large hyperscaler cloud company and...

to answer that question it's gonna be different within 10 minutes. So and there's no N/A. You can't just say this is not applicable to us so you have to put an answer in there and it's kind of like well do you just put something in there and this is going to be wrong in the next 10 minutes or what what we do with that. And then roles, of each individual working within the environment. We have thousands of thousands of thousands of people working within the cloud at one
time. So providing that information

and plus that changes too literally on a
daily basis, so providing that

information for ... how they want it, is
kind of an implementation challenge

that we are still working through.

And with that, it had not been all
horrible!

It hasn't been all just challenges. We have
some successes: we were the first

obviously, with Telos, to provide the SSP
to FedRAMP, which is good because now we

got the ball rolling on ironing out some
of the template issues, ironing out some

of the schemas and and learning
ourselves what we need to do on our side

to make this very successful and be able
to provide some of that feedback to

industry partners and kind of continue
pushing the ball down the road.
And we've also partnered with Accenture 3PAO to pilot the first pilot OSCAL authorization package for some of our services. And we are going to provide the System Assessment Plan (SAP) and System Assessment Report (SAR) to provide a complete OSCAL Authorization Package to the FedRAMP JAB.

And we hope to do that by Q4 of this year.

And some of the roadmap items right now:
-- We have the ... complete SSP again
-- We're working on this SAP the SAR and the POA&M -- We hope to have everything wrapped up by Q4 2022 to be able to really be pushing this forward out in a usable way that can be ingested by our customers.

And with that, I'm going to send it over to Stephanie to discuss some of our ...
some of XACTA's lessons learned as well.

So Telos has a solution that's called XACTA and we help manage our customers going through the RMF process and how they can get accredited.

But with OSCAL, we had to address some challenges where our models and our methods needed to be realigned to be able to export to an OSCAL package.

So we have a data exchange model, XDE, but we needed to be able to translate the information within XDE into the OSCAL structure.

and also make sure that we identify... I apologize for interrupting you. You are
sharing the presenter's view. I don't know if that is your intent. The swap displays button at the top. There! Yeah, there you go!

So we have a data machines model and it predates OSCAL, and then it was a way for us to export and ingest information between our XACTA solutions, but we needed to figure out how to get our XDE into, or convert it into, an OSCAL format. But then also make sure that we can support and balance future deployments of our scale that don't necessarily follow the FedRAMP use case and we also have to be able to ingest these manual documents that are being
provided to us, put it into our tool so that we can format it and convert it into OSCAL

so one of the first things that we did was leverage both our APIs

our forum posts and various technologies to ingest our handwritten SSPs, manual POA&M, spreadsheets and data

that's provided to the customer to get it into XACTA, so that we can output the information.

What we also found was our original FedRAMP template while in line with the original FedRAMP SSP, it needed some tweaks and modernization to be able to output into the correct OSCAL format
We were able to do some modernization of our template to meet the OSCAL requirements and then leverage the validation schema to output our OSCAL SSP.

And what we found was we want to be able to add new API endpoints and new calls to be able to not just output but ingest some additional OSCAL information especially as the model matures more and there are additional catalog pieces and customer information that we need to be able to pull into XACTA.

We've also worked with NIST and FedRAMP to create a feedback loop process just...
to address unique challenges or use cases that fall within these areas to
make sure we're still meeting the core requirements of NIST OSCAL
while addressing the unique use cases of FedRAMP
And leveraging the catalogs provided by this to make sure that we are
matching the information up with the core base model
so our future OSCAL deliverables and development are underway. So we're
working now towards outputting the POA&M model.
We're also exploring catalog and profile generation for our regulations that we have inside XACTA that are not 800-53 based
That way we can support customers who need to meet other regulations
and want to be able to use the OSCAL models

and we're also right now conducting analysis for SAP and SAR models to make sure we can output the full OSCAL package.

I think that's everything

That's fantastic thank you. Thank you so much. So if this is the end of the presentation, with your permission, I'm going to stop the recording.