Molly Wyatt: This is Session 23 which is the Improving the School Eligibility Application Process with the Integrated Partner Management Solution. My name is Molly Wyatt. I am the Program Manager for the project, and I'm the Director of the Technical and Business Support Services Group within Program Compliance. My colleague here is Susan Stallard who also is in the organization as the Project Manager for the project. So, first, let me ask those who were here in 2007, Las Vegas FSA Conference? Great. Who was here in 2007 and went to the IPM session? Oh, got a couple. Well, it's the same project, okay? Like we do in the government, we keep doing it, and keep doing it, and keep doing it till we finally get it right. Okay. Well, we're gonna get it right this time. All right.

So, let me, just as an overview, I'm gonna kinda start with just an overview of the project itself, and what it entails, and what it encompasses, some of the benefits of IPM, both from the government's perspective and from your perspective 'cause this product is for you, some of the roles and responsibilities of the project. You know, what are we gonna do with data? Obviously, we are just a plethora of data, and we are so good at it. We put it everywhere, and we duplicate it, and we do it over and over again. Well, we're gonna put everything in one place and only do it once.

We're gonna talk a little bit about how we're gonna continue to do outreach to the community, information sharing, make sure you guys know what's coming, and we do promise to train you before we implement. Isn't that great? That'd be really great. Four to six weeks prior to implementation we will train you, and the training will be very specific to the functions that you'll be doing. And I'll very briefly talk on a timeline because if I really told you what the timeline was I'd be lying 'cause it continues to shift a little bit, so we don't want to overcommit ourselves. So, hopefully, you will not have a problem if I don't read off the PowerPoint. Amen. 'Cause I just can't do that. It just kinda makes me weird. I just can't do it. All right. So, with that being said, we're gonna start with an overview.

IPM is probably Federal Student Aid's first initiative to actually integrate, migrate and enhance the Legacy systems that we're doing for Title IV eligibility and enrollment and oversight for Federal Student Aid. It is basically going to reengineer and replace five of our current Legacy systems. I'm sure most of you are familiar with the eApp. I know you love it, right? It looks like a big, long piece of paper on the screens. So, we will be replacing that, and I'll get into a little detail as to what we're expecting the

solution to do for you for that.

We're gonna be replacing the LAP which most of you will not have and don't have and probably will never use in the future is the Lender Application for those – and we no longer are doing FELL, but we are still using those partners as far as the servicing. So, we will still be incorporating that but nothing that the school institutions would be involved in. eZ-Audit, how many use eZ-Audit today? Have you been in the lab? Do you like it? Eh, it's okay. We're gonna be replacing that as well. PEPS, the Postsecondary Education Participant System is really our workhorse in the background. You probably don't have a lot of, you know, exposure to that application. It's actually the underpinnings of all eApp and eZ-Audit, as a matter of fact, and it houses all of the eligibility and oversight information that we do within Program Compliance.

And then we have a stovepipe system we called Electronic Records Management, ERM for short, which is our repository for our electronic images, paper products; we do scanning and have that, and again, it's very stovepipe. So, if you want to go look at a document, you have to go over there. If you want to look at the eApp, you have to go over there. If you want to look at oversight, you go over there, and if you want eZ-Audit, you go somewhere else, and you have an ID and password for every one of those. Okay. All that's gonna go away. We are going to have one integrated system for all of eligibility, oversight and enrollment.

So, let's talk a little bit about eApp 'cause I'm sure that's your all's biggest – well, eApp and eZ-Audit we'll spend a little bit of time on of how that is being impacted by IPM. First of all, we'll be going to simplified sign-on, as I've mentioned. There's only one ID and password, and once you get that ID and password within IPM, you will be able to use that same ID and password through several other systems within Federal Student Aid, for instance, Participation Management. I'll talk a little bit about that. We'll be eliminating you having to sign up for – well, you'll have to sign up for services within PM, but you won't have to have a new password, a new authentication, a wet signature and all that kinda stuff. That will be upfront for you as part of the eligibility process.

Very consistent user experience – our expectation is it's a very web-based application. We are using a SharePoint K2 platform. Hopefully, you guys are probably familiar with that. It's a Microsoft product, so it incorporates all the Word, all the other products for Microsoft. It's gonna have an inherent upload

capability, so we're going completely paperless with IPM. All of your documents that you're currently having to lick a stamp, put in the mail, FedEx, will all be – you can PDF it. You can Word it. You can Excel it, and it'll upload it directly into the system, and it will go into the doc management application, be actually attached to you for that product. That way you have one place to see all your information.

The other thing that it will be doing is looking like normal websites that you're used to going to, right? It's gonna have navigation. It's gonna have tabs. The application itself will be very intuitive as to who you are and what you're coming in to do for your particular activity. So, somebody asked me earlier about the re-cert. If it's time for you to re-cert – and one of the other capabilities of the solution or the expectation is we're gonna be reminding you. Your audit's due in 30 days. You're coming up for re-cert in 45 days. You know, you're really getting close; you've got 15 days. So, we have some alerts built into the solution so that it will help prompt you. You'll have your own homepage to where you can put your own links on it if you want to and kinda customize it to yourself, but it will have a specific workbench on it for you so it will tell you what we're looking for you to do.

So, if you come in as a re-cert, as an example, it's gonna ask you for what you're doing. And so, for the re-cert it's gonna come up, and the application will actually be catered to tell you the questions it's looking for you to answer. It's gonna tell you the documents we're expecting for you to upload, if it's required, and it's gonna show you what the current status and we call it a summary of your particular institution that you're working for at the point of re-cert. So, you have all of that at your fingertips, and again, it'll be very intuitive. It will be something kludgy. It will have a lot of help text on it, give you definitions so that you you're used to seeing and not something that's don't have to guess as to what we're trying to do. Once that you submit that activity, we will actually tell you where it is in the process. We got your submission. It's under review. It's been approved. Here's the next step. And so, you'll actually see how it's going through the oversight process.

It's a single-entry point. It will have some public areas on the website. I don't know if most people are aware; we do post the PEPS school eligibility file weekly out to a public site. This site will have that same access to public data that we provide today through some of the Legacy systems, and then we're really trying to enhance the security. Let me give you an analogy. eApp was built in 1998. PEPS was built in 1999. Now, think back in your

collective memory of the cell phone, right? Early to mid-90s, you're sitting in your car, and there's this platter-sized device under your seat, right? Emitting, you know, who knows the damage it did, right? And just, you know, to give you a perspective, the phone looked like this, right? Yeah, it didn't work too good, but it's what you had, right? So, you made it work for what you had.

This is where we're going with IPM. In fact, this is probably an old one, so we're probably going to, like, the iPhone or whatever the new technology is. We're trying to make this not only very, very secure, but also very easy to use to your benefit and to the benefit of the government. For those that went to the session this morning, you heard from the OIG. I mean, they are on us like, eeh, you know, just all the time. So, when they're looking at ways that we're trying to improve, and we are trying to safeguard fraud and abuse. Our Legacy systems are just not built to the security that we need today. Who went to the Two-Factors over the last couple of days? I was actually locked out on the first one. This will incorporate that technology.

When you have that token – let me just touch a little bit on what happens if you're a new institution. If you're a new institution and you're coming in for your first set of eligibility, we have incorporated the DPA as part of the application. So, the first thing you're going to be doing is telling us who your DPA is, and you're not going to be doing it based on – you're gonna give us your name. All the PI information will be very secure in that. Once you give us an e-mail address, the system will send and notify you, say come in and give us the rest of your information. The DPAs today, I believe, when they sign up other users to work within that institution have to run around and say, "What's your social security number? What's your social security number?" That's not gonna happen. You guys are not gonna be responsible for privacy information for your other constituents.

So, what will happen is when the DPA comes in and says I want Tracy to work on our behalf to do COD. I'm making that up, right? So, Tracy Turner, e-mail address is tracy.home and blah-blah-blah-blah, give just the demographic information for that particular user. The system will then send an e-mail to Tracy and say, Tracy, come in here. Here's a link, and give us the rest of your information, date of birth, social security number, blah-blah-blah – whatever else we need – and then that is secured and only pertains to that particular individual. We cannot do that on our current Legacy systems.

The other thing that happens with that enhancement is we have e-signature implemented as part of this solution so that when the DPA is put on the application, and the official come in to e-sign that this is all the right information on this application, and I give authority to that DPA to do work on our behalf, that e-signature then authorizes that DPA's authority. That same information will be transferred to PM, and you will not have to do that again within Participation Management. You'll come in with the same ID and password that IPM will be issuing you, and then when you go to PM, you put that in; they'll know your DPA because we told them you were, and then they'll basically say here's the services that you can sign up to do. So, I think that's really great.

Now, I know we had a question yesterday about, well, our officials will not go in and e-sign. Well, if you talk to our CIO he will, but there's also the ability to delegate the e-signature. The official does have the ability to delegate e-signature authority to another individual, but it doesn't relieve the official from the responsibility of the contract, all right? So, we are eliminating wet signatures. From the PPA perspective, that is also electronic. When that PPA is produced, it will be electronically shipped back and forth between the institution and Federal Student Aid to sign and cosign, and then you can print it off and keep a copy if you like, or it's inherent in the system and you can always bring it back up. It's always all electronic.

Okay. So, for those who aren't new institutions, you're probably wondering what about me? Well, I kinda mentioned about the data. We are expecting when you come in Day 1 into IPM, all the data that we already have on you, all the data we know about you, will already be in the system. We will be taking all of the – for instance, user information that we have from PM, from our current Legacy systems, and building a new user interface that we'll know whether you're a DPA somewhere, and we'll already give you that designation. You have a wet signature, as an example, within PM, and we'll keep that note on the system so that you won't have to redo that. We may have to be reaching out to you 'cause we don't have social security numbers for everyone, and so we may be reaching out saying, you know, we know who you are, but can you come in and give us your PII information so that we can store that? And we'll do that individually and not go back to the DPA and say we need you to go recollect those; we'll collect those individually from the things.

Now, you'll see from the diagram in the slide all the Legacy

systems that we're basically consolidating into one database, and we're normalizing it. We're making sure that we don't have redundant data. We're making sure the data that we keep is the right and the most current data. So, we're doing a lot of cleansing and that type of stuff as part of the data migration. The only thing we're getting from COD – we are not taking COD, okay? We are not at a borrower level; we're at a partner-level information. The only thing we're getting from COD is the RID, the Routing ID, which COD – I think they may call it the loan number or something within COD. What IPM will be doing is implementing a RID which is a unique identifier across all of our partners. Right now, we have Legacy identifiers. We have COD identifiers at a loan level. And so, we are going to be keeping and continuing to produce those Legacy identifiers, but we will also be including a RID that will end up, hopefully at some point, being "the" unique identifier for all of our partner organizations.

So, after we get all of that implemented, and actually, we are currently in the design phase; we are doing some core development at this point. All of our requirements are complete, so we are still moving forward. So, we will be trying to go out to more conferences, you know, Inshelp, NSAPS and all of those other types of institutional. So, if anybody wants to invite us, just let us know; we'd be glad to come, and we really want to talk and get this message out and get your feedback as to what you think. Our requirements are locked down, but if there's something that's inherent that you don't hear or if you have a question about, we definitely want to try to accommodate that. Then, again, training we'll be doing four to six weeks prior to implementation, and it will be very focused. We are taking – if anybody wants to volunteer for testing in UAT, you know, we'd definitely take those suggestions as well.

So, I very briefly touched on the timeline. What we're looking at right now is probably Spring of 2013 for the implementation. In the original project, we were doing a two-phased approach. Phase 1 was the eligibility enrollment, and then Phase 2 was the oversight. This time we're doing a one-implementation approach. Everything comes up live at the first implementation, and then we don't have this issue of trying to keep the Legacy systems in sync. So, we call it a big bang kind of effort that we're doing. Hopefully, the product that we're using makes it nimble enough that we can get that finished. So, somewhere between January and March of 2013 is a pretty good target.

So, I'd like to thank Sue. She did a great job of flipping those

slides, trying to keep up with me, 'cause I didn't probably look at one of them, and again, here's our contact information if you have any questions, concerns or whatever, and at this point, I'll open it up for questions, and if you could please come up to the mics, if you're taking back there I'll here, "Wah-wah-wah-wah." So, any questions? Well, I must have been awesome. Okay. Well, thank you for coming, and again, if you have any questions/comments, you can come up. We're available for, you know, till whenever, and thank you for coming, and don't forget to fill out the evaluation forms when you get the e-mail – Session 23. Thank you.

[Applause]

For those who hung around, now you're stuck, okay, 'cause I'm gonna talk some more. I forgot to mention about the DPA 'cause I know you guys – the DPA role is changing with IPM, okay? It's changing in regards that it has a much more high – thank you for asking, by the way, 'cause I totally forgot. Tell them we said hi. Anyway, it has a much more heightened security requirement. Now, I mentioned that you're not gonna have to gather social security, but you will be responsible for anybody that you sign up as a user to make sure they get security training, that they're following the rules, because ultimately, the DPA is responsible.

And so, what I was asked yesterday if I could look into is we are going to put together, if you want to call it a slick sheet or some sort of document that outlines what is the definition of a DPA? What's the roles and responsibilities? What are they allowed to do in each of the systems that there is a designated DPA? Within IPM, there are DPAs which we call primary which are done as part of the application, and they do a e-sign, right? And then there are what we call secondary DPAs that the DPA can go in and assign additional DPAs so that they can do work around other parts of the business process. So, for instance, they may sign a user up at a location of a school so that they can sign up users to do work within that location, right? Or the DPA can do all of it. So, they can assign secondary DPAs to help in the workload. The only thing the secondary DPA cannot do is assign another DPA, but they can sign up users, right?

In the participation management world, that primary DPA will be considered the primary DPA to signing up for services, and then that secondary DPA would be considered just a regular PM user so they can get a mailbox, as an example. So, I'm gonna try to put that together, getting business operations to tell me how they're

expecting to use a DPA, but all of that signing up of those initial users from a DPA perspective will all be done through user management and IPM. Does that kinda answer your question? 'Cause I really cannot tell you standing here today what PM does with all of that kind of stuff. I do know that they use the DPA definition a little differently than how it's gonna be used once IPM rolls out because they're not going to be doing e-sign. I mean, they're not gonna be doing wet signatures and all that other kind of stuff. So, I think some of that will be changing, and I'll work with them to get something put together so it's very clear for you guys when you kinda go forward. Yes, ma'am.

Audience: *[Off mic]*

Molly Wyatt: Yes to all. We're gonna have CDs. We're actually gonna have a training site once we can ever get it put together. We'll have a training site where you come in and practice, as an example, once it gets implemented. We're going to look at webinars, and we're gonna partner with the training offices that currently go out to do training to our partners. So, we'll partner with them to figure out, you know, what are the best avenues? We're gonna have the materials built very specifically to the function. So, for instance, if you're a financial aid director, what do you need to do in IPM to do your job?

If you are an auditor, as an example, and you're coming in and you have the designation to do uploads of the financial statement compliance audits, as an example, here's what you need to do, and here's all the places that you need to go with the basic understanding of here how you navigate through the system in general. So, we'll do webinars. Like I say, we're trying to reach out to go to some of the conferences to get the message out. Once we get closer to something that we can actually show – we'll probably be here next year. Hopefully, there won't be 7,500 people, maybe 8,000, right? And try to do some hands-on training once we can get something in the hands of people to use so, yes.

Audience: *[Off mic]*

Molly Wyatt: Yes, you would. So, you'd go into user management, and you designate that auditor – they're basically supplying a service for you, right? So, you would give that person, that individual, authority to do uploads of your financial statement compliance audit. They'd come in, give their credentials 'cause all you'd give is the name and e-mail address and say what the affiliation is. IPM will also keep track of all of the affiliations an institution has, all

the locations it's affiliated with, the auditors they're affiliated with, if they happen to have a third-party servicer or any kind of that stuff will all be part of the partner view to where you can see all the people that you're doing business with. And so, you would designate that person to do that kind of upload, and then they come in and give the information, and then they get access to that particular part of the solution to do the audits and financial statements.

Audience: *[Off mic]*

Molly Wyatt: It's very dynamic, yeah. It takes as long as you going in and deactivating one, adding the next one, and the e-mail going to the new one. So, as soon as they come in, they get their credentials, they're good to go. So, I apologize; I kinda missed that little tidbit. Is there any other questions? Good questions, no questions are dumb.

Audience: *[Off mic]*

Molly Wyatt: Well, we won't send any privacy information through e-mail.

Audience: *[Off mic]*

Molly Wyatt: The question was if we are sending e-mails with a link to tell you to come in and give us your privacy information, how are we preventing phishing at your end?

Audience: *[Off mic]*

Molly Wyatt: You know, I don't know. Take that note. Yeah, we have it. We will be using – you know, since we're using SharePoint Microsoft, we'll probably be using Outlook to send that stuff out. So, it'll probably be going out as a – but I understand what you're saying. So, if you get a link that says come into FSA IPM, you know, how are you gonna know that that's really at the safe IPM, as an example?

Audience: *[Off mic]*

Molly Wyatt: Yes. Actually, that's a good point too, to your question of how immediate it is because if you went to the Two-Factor, right, each institution or whatever is being asked how many tokens do you need? I think, right?

Audience: *[Off mic]*

Molly Wyatt: If it was phishing, and they clicked on it, and it took you somewhere else, you're gonna know if you're not Two-Factor, you're not at FSA, all right? But to that point, if the institution wants to change the auditor, you've got the tokens, right? So, you have to get that token to that auditor before they could come in – they can come in and give us their privacy information, but they wouldn't be able to then come in and get authenticated until they got their token.

Audience: *[Off mic]*

Molly Wyatt: Oh, where's my token? Tracy's gonna speak to – I was gonna show you what the token looked like. All right. So, it's a magnifying glass. This is a Two-Factor token. It used to be a lot bigger. It used to be, like, square.

Tracy Turner: So, what's going to happen, Molly has a token. I'm Tracy Turner. I'm the Technology Office within FSA. Molly is showing you the token that will be distributed to every DPA by the end of 2012. So, the last schools will receive their tokens by December 31st, 2012. So, by the time we go live with IPM, everyone will have their tokens.

Audience: *[Off mic]*

Tracy Turner: Well, if you're using CPS, NSLDS and COD, then you will have to start using them as soon as you get your tokens, but for IPM, you will use it at the time we go live.

Molly Wyatt: Yeah, by the time we go live in early 2013 you should already have your tokens, but to the point of how fast it is, it's gonna be based on when they get their token, right? They can come in and give us their privacy information. We can send over and say, okay, come to this link now to login, but unless they have their token they won't be able to login.

Tracy Turner: And so, everyone will have their token prior to.

Audience: *[Off mic]*

Molly Wyatt: Okay. There's a random generated number. When you press the button the number comes up, and the number is based on when you registered – there's a registration number on the back which is how they know it's yours, and you register that number to your ID, and then there's some algorithm based on how – maybe it's the first

letter of your last name and the second letter of your twin brother; I don't know whatever all that kind of stuff is.

Tracy Turner: *[Laughter]* It's a randomly generated number.

Molly Wyatt: And then it generates a random number that is unique to your ID. So, it's Two-Factor saying I know you have the right token. You've given me your right ID and password. You must be who we think you are. That's how it works.

Tracy Turner: And just to add to that, the thought behind the security for Two-Factor is something that you have and something that you know. So, your single sign-on is something that you know: your user name and password. The something that you have will be the token that you're going to receive no later than the end of next year which will generate that ID number that you will insert when you enter your user name and password, and that will be your two methods of authentication.

Molly Wyatt: Yes, ma'am.

Audience: *[Off mic]*

Molly Wyatt: How would the auditor have the token? You're saying – oh, they changed personnel within that auditor's office?

Audience: *[Off mic]*

Molly Wyatt: No, the first time they get issued a token would be, I'm assuming, from the original – the first person that signs them up, right?

Tracy Turner: The DPA.

Molly Wyatt: So, and then you, as an institution, say I'm gonna say, you know, I'm gonna do business with that same auditing firm. That auditor's gonna come in – when you come into the system and say I'm gonna do business with this auditor, it's gonna be in a drop-down for you if we already know about them, and then you just have to pick them.

Audience: *[Off mic]*

Molly Wyatt: If they are already on the drop-down, they already have a token, and they already are in the system, and you just have to build an affiliation with them to say I give this auditor authority to do business on my behalf, and you sign them up as a user, and then

when they come in, they get the list of RIDs and OPE IDs, as an example, and say I do business with all these, and they pick whichever they're doing their work for, and then they go and do their work for that particular institution, yeah.

Tracy Turner: Now, this is going more into Two-Factor authentication and not so much IPM, but it is the responsibility of the DPA to issue the tokens to all of their users. That's not a function of IPM. That's actually the Two-Factor office. So, it's their responsibility, and the DPA is the one who has to have the updated list of users, whether it's third-party servicers or the other constituents on the campus. So, the DPA is the focal point.

Audience: *[Off mic]*

Molly Wyatt: You mean if they already exist?

Audience: Yeah.

Molly Wyatt: If they already exist, you don't need to know anything about them except their name so you know how to pick them out of a drop-down.

Audience: *[Off mic]*

Molly Wyatt: They're screwed.

Tracy Turner: Again, this is getting into the Two-Factor.

[Laughter]

This is IPM, not Two-Factor, but if they lose a token, you're gonna have to go back to the DPA.

Molly Wyatt: They'd have to go back to the DPA. They'd have to reissue. I don't know if they have to pay a deposit or whatever, and they'd have to be reissued a new number, a new token –

Tracy Turner: Right.

Molly Wyatt: – and they'd have to go back in and re-register this number with their ID. So, basically, they would replace their serial number with the new one.

Tracy Turner: That's correct.

Molly Wyatt: I know pretty much about it.

Audience: *[Off mic]*

Molly Wyatt: Well, again, since the DPA is really responsible for the users on their system –

Tracy Turner: Right.

Molly Wyatt: – if they know somebody has left, they need to go in and deactivate the user ID. There is auditing within the solution where it will do, you know, the 90-day check. If somebody hasn't logged on in 90 days, you know how that goes, they get suspended, and if they don't log in for 160 days, then we kick them out, but if you actually have a user that has left and you're replacing them, then the DPA is really responsible to manage those user relationships.

Audience: *[Off mic]*

Molly Wyatt: I don't know. The next Two-Factor session is at 9:00 tomorrow morning. I just looked. I don't think there's one today. I think there was one yesterday so 9:00 tomorrow morning.

Audience: *[Off mic]*

Molly Wyatt: Okay.

Audience: *[Off mic]*

Molly Wyatt: The token is yours; it's not the school's. So, you'll have the schools in your drop-down saying I'm responsible for these five schools. It has nothing to do with the token, but – what? Are you a servicer or you're at a school, right?

Audience: *[Off mic]*

Molly Wyatt: You're able to do that because the token is assigned to you, not any school in particular. Any other questions? Did I miss anything else, Sue? This is your last opportunity.

Okay. One of the other changes that we're making within IPM is that servicers – right now servicers can do – you know, they come in and sign up themselves, right? And say we're gonna do whatever we're gonna do. That's gonna be eliminated with IPM. For a servicer to come in and do business, the school has to give them access. So, in other words, the school has to establish that

relationship, and the servicers will be in a drop-down, if we know about them; you can pick them and say this servicer now is going to come in and fill out my application, or they're gonna come in and do whatever. So, it has to actually be initiated by the school to make those relationships happen before they can come in. They can't sign up themselves anymore. That's all being eliminated, but those that currently exist will already be part of the system when we come up live so they won't have to redo that.