B. Hampden: Thank you, Linda. I'm sure you would agree that we needed that pep-up because we're probably either full of sugar or very hungry and tired. So, let's try and make this as interactive as possible, even though I'm gonna ask you to hold your questions until the end so we can get through this. I am – I guess I'll consider myself a newbie to FSA because I've only been there for three years. But the first conference I attended, I could not believe the groundswell of emotion around sign-on and how many different permutations of sign-on that individuals had. And I thought to myself, "I cannot have anything to do with technology and not work on a solution." So, I feel very, very proud to be able to have this session with you, to let you know what we're doing, and to really let you know that, in fact, we heard you. So, we're gonna go through a program that we have just initiated at FSA that is meant to tackle the identity management initiative. I hope you're not – okay. It's something that's clearly bigger than a breadbox. So, we have decided that we are going to approach it in chunks. We will go through this presentation, show you what we're doing, kind of elicit from you any ideas you may have. But more importantly, the message that you should have after you leave here is that we have heard you.

As I said, the frustration is the number of sign-ons that all of you have got to be – have got to carry around to get into all of FSA's systems. Each one of them is different because as you well know, over time, we have partnered with a number of individuals, a number of companies to help build solutions. Each one of them had their own rules around how they wanted to design the logon features. So, you all were the recipients of all of that lovely technology which only meant that every permutation meant a different ID and password combination. EIMS is meant to provide for you the vehicle that allows for single _____ sign on for a number of your applications. That – this chart here is, as you know, very important as it depicts for you the number of permutations that you have. If you look on the left-hand side, you see where we're talking about just three applications. For some of you, you've got five, six, seven user ID and password combinations – many of those for COD. If you are looking at managing the portfolios or managing the information for different schools, every one of those is a different combination and password. If you look at the middle box, you see those ID and passwords for some of what we call anchor accounts. So, that's where we are all heading, right? John Doe at FSA.

Then, of course, as I said, we've got many partners that we do business with. So, if you had to log onto MCS, you had another password. DLSS, you have still another password, and it goes on and on. Again, that only is focused on accessing our systems. When you add on everything else that you have – Amazon, your bank accounts, it becomes untenable. And so, the last session we had, people asked, "Well, how do you manage all of these passwords?" We can give you nice little tips, put them all in a file, don't name the file "password," protect the file. But at the end of the day, you still have 15 or 20 IDs. It is not the best thing for security. And remember, we look at that as the access point into all of our systems. Over time, I don't think we've done a good enough job at solving this problem. So, that's what we have today. What we are trying to do with this initiative – EIMS stands for Enterprise Identity Management System – is to provide for you the ability to register once and have access to systems as the need arises. Clearly, we're not gonna open the kingdom to you. So, you still have to have a reason, and as part of your job functions, be able to be qualified to have access. But, it is important for us as we build tools that will enable this access, and as we build mechanisms that allow us to know who you are, it is important for us to have this one stop shop, as I would like to call it. So, what we're trying to do is to create a standard method for supporting our entire FSA portfolio of systems. We're also looking to remove all of the PII information. So, as you know, students who login use their social security number. That is clearly not something we should be doing in this day and age. I don't need, necessarily, to tell you why. But if you really need to know why, come to session 30. We'll go through all of that and we'll tell you why it's not good. But, it is very important for us, if we're going to be the purveyors of all of the security around the protection of millions and millions of identities, that we remove social security number, date of birth from our login systems.

That will allow us, if we can accomplish those things, to have that – as I said, that's standard process across all of the systems. What we're going to do to begin is: we're utilizing an authentication system that we call AIMS, and it's pretty simple – Access and Identity Management System. That will be the system around which we will build our security. So, any one of the legacy FSA applications will be connected to AIMS. You, as a user, will be authenticated through AIMS, and then based on the credentials that you have, you will be directed to the applications that you need to get access to. So, AIMS will be that frontend that we will use, and then of course, we'll go through all of the other systems. We will also be using leveraging PM – participation management – to enable the COD enrollments. Then, as a further step, we will be creating a standard ID that would allow us to authenticate and identify all of the users. And then, the last phase of this will be the removal of the token. So, for those if you in the room who we call privileged users – and that goes for many of you here because you are FSA – just had a mental block, but you are financial administrators, and so you, for us, are the privileged users since you have access to information more than your own. The other group of people, of course, are the non-privileged users, and those are all of the 70 million students who come into access just their own information. Right now, all of you – show of hands; how many of you are using the tokens that we gave? Oh, wonderful. I know you probably hate us, but that's all right. So, all of you are all privileged users. The next phase of the technology that we want to implement is, of course, the removal of those, because those have a shelf-life of about five years. And so, in five years, we don't want to put you through the stress of having to swap out all of those tokens. We don't want to go through the hassle of mailing you all of those tokens. So, we want to take advantage of the technology, which is using self-tokens.

Now, this is not going to be accomplished overnight. This is a program. We're in this for the long haul. There are a number of pieces to this. When you look at the timeframe, we're looking at the next four years – somewhere finishing in 2016, even though it says 2015 there. 'Cause there are other pieces that I haven't talked to you about, but I will as we go through this presentation. Where we are today is on the left-hand side. You've got the privileged users and non-privileged users. At the end of the day, they all come into our FSA systems using different methods of authentication. Where we want to get to is: looking at the community much more holistically, but not reducing the requirement for security as it is appropriate. So, when we're done with this, everybody will have a single FSA ID that will allow them to access all of the systems as is required. Okay?

When we look at the identity management space, this is what the picture will look like. In the middle there, the mustard color, you see our identity management service. That's the engine that will drive how we connect to the backend systems. What you need access to will be held in that engine. How you get it will also be held in that engine. There will be different ways of identifying how you get there, but most of the effort will be done in the background. So, it will be transparent to you, and that's the goal here: to have you sign on once, have access to multiple applications.

Okay, there are two major systems that we're gonna talk about today: COD and PM. In the audience, I have help, 'cause I need help. These are our great partners – Accenture and Vangent – are both here to help answer any questions that might come up. But these are two of our very important partners that we use to ensure that we are delivering student aid, and they play a very critical role. So, as we go through – I'm not going to stand up here and suggest to you that I have all the answers, but I have Eric, and I have Stacy, and Tiffany, who will help me navigate once the question and answer session comes in. Currently, the primary DPA enrolls users through COD. When we are finished with our first phase of this enhancement, the primary user will go through PM to enroll the users into COD. Additionally, users receive different logins as you know. This is why the first slide I showed you had so many permutations. Different logins based on the schools that they're supporting. Going forward, in – for the COD application, you will have one login, regardless of how many schools you are supporting.

Also, users need to log out to go into the various schools that they have when they're changing schools or profiles. Going forward, you will not need to do that. So, are you guys getting excited about what I'm saying here? But I think, you know, I know that you will agree with me that this has got to change your life going forward. Users only have to access the reports created for specific school – going forward, you'll have the ability, again based on your need, to be able to access all reports for the schools.

Currently, PM does not provision enrollments for COD. But, going forward, that's one of the differences that you will see. We will use PM because that, again, is the system where we want to collect all of the information around our participants so that we know about everything in one system, rather than having it spread all over. That's been – that's actually been something that we've noticed. Even as we look at the new release of IPM, that is another phase for us: to be able to look at what's in PM, what's in COD, what's in IPM and determine where it should fit so that it is in one place. But that's also going to come later. Primarily DPAs also have to enter user and enrollment information into multiple systems. Going forward, you're gonna do it once, which is in PM. It will permeate throughout all of the FSA systems: COD, NSLDS, et cetera. Right now, PM is not linked to AIMS for the COD online. Going forward, it will be. Right now, many of you have AIMS or access your systems through AIMS. So like, NSLDS and some of the others – COD is the last lagger that we're gonna put behind AIMS, and we're gonna do that through PM.

So, the way this is going to work: we are in the process of doing the systems modifications as we speak. We are hopeful that by the end of the first quarter, we would have a majority of the modifications then. So, between March and the first week in May, we are going to begin a series of communications with you to get you ready for the ultimate cutover, which will happen in May. We will start by asking that the primary DPAs enroll into the current COD online systems – enroll all of those users in PM. We'll also ask that the users will register in PM if they do not have an FSA ID. Some of you already have an FSA ID. We will just use that FSA ID and link it. During that period, also, any new COD users will need to be enrolled in both systems because we are at that point – still running in parallel. After that, the first week of May, then we'll only be – the primary DPAs will only be required to go through PM to be able to enroll any COD online users. So, a little bit of the pain for the new COD users will be that you'll have to enroll in both systems, but that's just for a very short and distinct period of time. So hopefully you'll bear with us through that.

So, in terms of the changes that we're talking about: currently, you have ABC.FSA. Between March and May, you'll go ahead and you'll enroll in both – enroll users for COD online through PM. You'll – if you're using a token, you don't need to do anything. A lot of that work has already been done for you. If you don't' have a token, the existing COD online users will need to get a token, and I believe most of you will have a token. But then, there's still those who had not been given a token until now, but you know, we have plenty of tokens that we can give out. So, not to worry. The primary DPA user will enroll in the COD online access through PM. New COD users, as I said, will have to continue to do both during the months of March to May; but then, you'll also use that same token.

Now, the other thing we're doing is taking this opportunity to enhance our privacy and security posture across the board. So, one of our requirements is that you have to accept the responsibility regarding how you use FSA systems. We want you to understand that it is a privilege to be able to access the data that's in our systems, and you have a responsibility to protect the integrity of that data. That is done through the rules of behavior document that is online. We will now require that you sign that. You read it and sign it – electronically, of course -- and we will keep track of that in PM. In addition, FISMA requires that we track and report on that information. So, we will have it. Each day that you access the system for COD, you will be asked to accept these statements. So, it's a one-time thing every time that you access the system. It's like you do anyway right now for, hopefully, many of your systems. So, we will be capturing that information. And in addition, as you know, before you have been granted access to the systems, you are required to go through the security awareness training – the annual training. We are going to now automate that process, so annually you will be required to renew. You will be prompted ten days before the expiration date, and you will be prompted every day for ten days to go in and do the course. On the 11th day, if you have not done the course, don't be surprised because you won't have access. So, don't call; just go in and do the course, all right? Very, very important. We will automatically disable the account, so don't call your help desk. Just remember that Bridget-Anne told you this back in November of 2012.

Now, just a pictorial: we'll register you through PM; you get the ID. You will then enter the FSA ID and password to get into COD. COD will then check to see if you had done your security training. If you have not done it, it will not allow you to go in, so it'll send you back. You will do that training, and then with a positive affirmation, you will be allowed into the system.

So, important dates to remember: we will begin to publish communication on the ______ website in February. During the months of March and May, we will go through and detail for you exactly what you have to do. We're not going to leave you out there hanging. We'll walk through this step by step with you. The important thing is that the DPA will have to enroll the COD users in PM. Then, the COD user will be asked to go in and register, and create a profile in PM, and get the new FSA ID and password. During the first week of May, you will then be able to log into COD and you will, only at that point, have one user ID and password to remember for all of FSA systems.

Are you clapping? You can clap harder, 'cause – so, that's the phase one and two that we're working diligently on to complete. We have other phases that we are partnering with. So, once we go through and we are finished in the first week of May, we will then proceed to work on removing the PII information from the systems. That work is beginning now and will go into 2014. But by then, we're hoping that we will be able to remove the social security number, date of birth. We will also be allowing you to change your ID and password, as opposed to having to make a call to the help desk to do that – very much like any of the standard sites that you get into now if you've lost your password or you forgot it. They send you a link, you go in and you change it. That's where we're going with that. Additionally, we are working with the education community in an initiative called In Common, where we're looking to standardize the use of ID and passwords across the education space. So, here again, the same ID – the thought is the same ID that you would use to get into some of the FSA systems could be used to get into other universities – if the need or the network is in place to do that. So, we're actively partnering with this group called In Common so that we can be on the forefront of ensuring that we have the access and identity management process as clearly defined as possible.

Additionally, we're part of a group of six or seven federal agencies that have begun an initiative, and it's actually now being put into the proof of concept phase where we want to be able to authenticate a user, credential that user using some of the larger credentialing outfits like Google, like Experian. That ID and password, once credentialed, will allow that individual to get into multiple agencies. So, if you needed to get into social security or IRS and then come and swing around to the education, you can then be allowed in based, again, on your level of authority. So, there's some good work going on there, which I think is very good for the public to be able to link us together as the government. Of course, as you can well imagine, there are a lot of checkpoints that we're going through to make sure that we can, in fact, authenticate who you are and ensure that you can get to the right data, ensure that if something happens and your credentials are compromised, we can easily cut it off. We're going through that pilot right now to work out those kinks. But at the end of the day, the message here for you is to remember that federal student aid is diligently pursuing this initiative because we understand the complexity, we understand the inconvenience that you all have gone through year after year after year, and it is incumbent on us to find the solutions that make your life a lot easier when it comes to protecting PII data.

So, I will stop here, and I will ask for questions, if there are any. There are some mics. There's a roving mic, also – if you have any. Sure.

Audience: *[Inaudible]*

B. Hampden: The tokens. That's a plant. She's a plant. She's actually – stand up. Yes, stand up. This is Dr. Linda Wilbanks. She is the chief information security officer for Federal Student Aid. She has joined us from NCIS, where she was the CIO, but she has spent a lot of time in security. So, she's asking me a question: where do we get the tokens from? The tokens, of course, come from FSA.

So, for any of you who do not have a token – and I don't think any of you in this room. Does anybody not have a token? See me after. But you apply for tokens through FSA, and I'll get you all of that information. Yes, sir?

Audience: Hi. I'm the DPA for my school, and I really appreciate all the efforts that you're making to make things simpler both for the DPAs of the world and for the other financial aid officers. So, I think based on what you said, my understanding is that this new participation management site will be replacing the current SAIG enrollment site as the one that DPAs use to manage users?

B. Hampden: All right. Anybody – no?

Male: *[Inaudible]*

B. Hampden: Why don't you give him the mic?

Male: No, it's just a new service that you'll have. You know how when you go in and you enroll for different services? It's just going to be a new service that you have as an option. And then also, I guess the best way – the easiest way, if you're already enrolled, when you go to that secondary – that DPA – your primary DPA page where you have the four different options, and in the top right hand corner you've got your ________? It's actually going to be up in there. So, it's going to be nice and easy for you to go and click. We're changing that section. That was an NSLDS online user section. We're actually changing that so now it's going to be just your online users. You're gonna have your NSLDS, also your COD online.

Audience: Okay, great. I think that makes sense. And then, my other question is: as a DPA, some of the other frustrations that we have have to do with the requirement of creating a separate TG number for each individual NSLDS user, which is both – which is confusing. I'm wondering whether this PM system will change anything to do with the TG setup, the TG box setup, or the way that we sign up users to participate. For example, all the signature pages that we have to do and mail in for NSLDS users, and the signature pages that we have to maintain for users of the FAA access to CPS, et cetera.

B. Hampden: Wouldn't some of that go into PM? Because I think that's what we're trying to do, right? We're putting all of that – I told him to come up here and sit. He didn't want to do it.

Male: It’s actually gonna stay the same. There will be more as you had indicated: in February, there’s going to be more guidance on the signatures and what’s actually going to be required. If you’re already signed up for the COD batch, I believe the signatures – we don’t need to have the signatures. I don’t remember for sure, but the information that comes out in ______ in February will have all of that.

Audience: Okay. It sounds like it’s not going to simplify things for NSLDS.

Male: Not at this time.

Audience: Okay. All right, thanks.

B. Hampden: Any other questions?

Audience: *[Inaudible]*

B. Hampden: No, that’s separate. That’s separate, but we are doing – we are looking at some of those enhancements; but no, it’s not part of this. But at the end of the day, any of the applications that you are trying to access, you will go through AIMS. So, the intent is to put everything behind AIMS so you just need one logon. ID. So, we’ll get there. We’re probably not there with EdConnect right now. Come see me after so I can get you a proper answer on dates and that kind of stuff – on that one. Any other questions? So, hopefully – yes?

Audience: *[Inaudible]*

B. Hampden: That should not have happened, because that’s what we’re saying. Once you do it, it should link. So, come see me after, and we’ll definitely figure out why that happened. But thanks – thanks for that. Hmmm. Yes?

Audience: I have a soft voice. So right before I left, one of my employees told me that if he does not clear his cookies, he can log on without having to use his token.

B. Hampden: If he does not clear what?

Audience: His cookies on his history of his computer. He can log on without having to use his token. He just goes into his bookmarks and gets into his – into FSA without having to use his token. And as the technology administrator of my school, I was required to follow all the rules that you guys set when you gave us our tokens, and we made sure everybody had activated them before Thanksgiving. So, that was kind of a concern for me.

B. Hampden: So, clearly –

Audience: And we've had IT look at it –

B. Hampden: So, clearly there's a session that's not actually logging off. So, I –

Audience: I just wondered if there was any – if anybody else had experienced – you know, these tokens are so new, I didn't know if anybody else had experienced that.

B. Hampden: Well, they're not that new, so – you know –

Audience: To us, they are. We were the third rollout.

B. Hampden: But in terms of the technology, yeah. Has anybody else had that problem in the room?

Audience: Oh yay, we're not alone.

B. Hampden: You've just vindicated her. Have you reported it? You gotta tell us. Okay. So, it's steve.burke@ed.gov. Okay? S-T-E-V-E dot B-U-R-K-E at E-D dot gov. Send him a little note. I will also tell him. There's my e-mail, in case you forget that other one. Send me a note, and I'll make sure. All of you who's having that problem, just send me a note and I'll make sure that we get that solved. Yes, ma'am?

Audience: Is the G5 system also going to be moved behind AIMS?

B. Hampden: That is coming. We are talking. They are actually looking at AIMS. They have begun to do their proof of concept. And so, the answer is "shortly." Questions? Going once, twice, three times. Finished. Thank you so much for your time, and please feel free to reach out to me. Actually, encourage some of your colleagues to come in and hear the good news. Thank you.

[End of Audio]