IRVIN HAYES JR: All right, welcome everyone. I hope you guys are having a good EU so far. although, it's just really the beginning. And welcome to Security Awakens. We're going to discuss today-- actually first before we talk about discussions, let's talk about who we are. So I'm your primary speaker today. My name is Irvin Hayes. I've been working with Autodesk for almost 12 years now.

Ever since I've started working at autodesk I've been in product support. I was a user experience designer, and now I'm a product manager over the product line. I've been working-- I have a background mostly in IT. Actually I'm not an engineer. I'm not a designer, but with an IT background. Many of you I have talked to you in the audience and I've helped you in a lot of your issues or configurations with setting up Vault. So that's where my strongest suit is. And with that, I'm going to introduce-- allow my coworker to introduce himself.

ANIL CHINTAMANENI: Hello everyone. My name is Anil Chintamaneni. I'm a user experience designer at Autodesk. I've been with Autodesk for almost 12 years like Irvin. I started out as a QA engineer and most of my tenure at Autodesk I've been focused on PDM products, mostly Vault. And prior to joining Autodesk I was in the automotive industry for a few years after school.

IRVIN HAYES JR: All right, so hopefully you read the class summary here. But what we're going to talk about today is security inside a Vault 2017. I'm going to give you some examples of what security was in 2016. I'm going to tell you how it changed and was enhanced in 2017. And then how you can actually use it when you go back to your office. So our key objectives here at is the end of this class you'll be able to configure object-based security, you'll be able to configure state-based security, you'll know or have the knowledge of using both the object-based security, and lifecycle, or state-based security together, and how they combine and work with each other. And then you'll know how your users are going to be affected by the security settings that you configure.

Now what you will not-- or what I will not address in this class is actually how you configure life cycles, all right. So this is all about security. I'm going to show you life cycles but I'm not going to tell you how do you actually set up the entire lifecycle to do various different workflows. It's all about security inside of Vault. So if that is not the class you thought you signed up for, you are free to go and find another class that you would like to visit. Other than that, we're going to jump right into security.

ANIL CHINTAMANENI: Also this class is covering Vault Work Group and Professional.

IRVIN HAYES JR: Right.

ANIL CHINTAMANENI: If your using Vault Basic this class is probably not for you.

IRVIN HAYES JR: Yeah. So actually, how many Vault Basic users are there? I talked to at least one gentleman who's in Basic Vault. A couple. Did you raise your hand?

ANIL CHINTAMANENI: Yes.

IRVIN HAYES JR: A bunch of Autodesk employees over here so you can bug them later. Vault Work Group. You're not the only one this time. You've got a couple more Work Group users. And everyone else is Professional. Anyone else on Vault, let's say 2016? So I talked to a few of you. Who's on Vault 2017? Who's on something earlier than 2016? All right, so all of you need to talk to me after class and we're going to upgrade here at EU.

AUDIENCE: We havea test.

IRVIN HAYES JR: You have a test sir? OK, so you're almost there. I'll let you slide, everyone else we're going to upgrade after class. So the key thing here with Vault Security is we've done some enhancements over the years based off of your needs or your requests. And we've made it more flexible in the new model Vault 2017. So this is what we're actually going to jump into. But I'm going to start off with some of the basics, especially for those who are in the class who understand or don't know about work group and professional and the current security models that you might have seen in 2016 and earlier. So I need to bring everyone up to speed to make sure you have the base level knowledge and then we're going to deep dive into it later so that everyone then sees the benefits of the new security model.

So the first thing we're going to cover is object-based security or the different objects security types. So we're going to talk about acronyms such as the access control lists, or ACL. So I'm going to start using abbreviations and if you don't remember the abbreviation just yell out and I'll repeat that. But access control list is just a basic list of users or groups that are assigned to an object-based. And you assign the security to that particular user or group.

Role-based security, we'll cover what role-based security is. We're going to cover-- then at that point we're going to cover what object-based security is. From there we're going to jump into state-based security. And then from there we're going to talk about the permissions. This is one of the things that you must know and understand is the precedence in which the permissions actually act. So deny will always take precedence over any allow or grant. So you have an allow permission and then you have what's called a no permission, or we call it actually null permission. I'll discuss what that is as well during the class here. So keep that in mind the precedents and how they work.

So let's jump in the roles. Are there any-- anyone in here using Vault but you're not an administrator? We get all the administrators in your, sweet. We'll throw you out, all right.

AUDIENCE: What's an administrator?

IRVIN HAYES JR: What's an administrator? So-- we really have to talk after class.

[LAUGHTER]

IRVIN HAYES JR: All right, so what are the roles. When Vault's installed we come out with a group of roles that you can assign to your users or groups. These roles are a-- we'll just call it a title that has a group of permissions that are assigned to that role. Your users, when assigned to that role are allowed to do whatever the role allows the user to do. So I'll give me some examples. There are much more roles than this. And actually, I forgot to upload it, but after class I will upload an Excel sheet into the additional handouts.

It's an Excel sheet of all the roles inside of Vault 2017 and then you can filter it based off of what the permission is. So that you can see him outside the Vault. I know the dialogue doesn't show you very well what the roles are and how they compare to each other. And it also shows you what addition the role actually starts in. All right, so I'll upload that Excel sheet later.

But when you're looking at roles, again, you have the basic document consumer, he has the read-only role. You have document editor level one, level two. These roles start to build on top of each other. So some of the roles you can use independently from each other. But in other roles, such as you have a document consumer, you have a document manager, you end up combining those two roles together, and then they have a super set of permissions inside of Vault.

So just like we're showing here, again combining the document consumer and a document editor level one, you're granted the least restrictive permissions within inside of Vault. So all the permissions that each of the roles give you, that's what you have. At a role-based security level, all right. Now this one's not really actually a great example, but document editor level one and if you combine it with like a Document Manager level one, you just have a super set of roles that you can use or assign to a group of users.

So when we jump out of roles-- so that's just the basic level. It starts in Vault Basic and works its way up. The higher you go up the more roles we will actually give you. But we want to talk about object-based security. So when we jump into object-based security there's a few things that you need to know as far as the permissions that you're allowed to give a user.

Read, modify, and delete-- and these are actually assigned to a particular object-based. It could be a file, a folder, we have custom objects in there, and these are the permissions that actually you end up setting on those. It is set by an ACL, remember the access control list the user, that's placed on the object-based. And then you will check some boxes-- or actually you'll hit a drop down which I'll demonstrate in a little bit and assign that user. So these are the basic permissions here, read, modifying, and delete. And you'll see that throughout when I show start showing you some demos.

Folder security has the same thing. So it has its permissions, rewrite, modify. Within a folder it actually grants you other things as far as the files within those folders. So if I can read the folder I can also read the files within the folder as long as they don't have different permissions set on them. I can then modify the folder. I could modify the contents of the folder, which is the files and the subfolder within it, or then in this case, I can delete it as well depending on the permissions.

Most restrictive applies now when you are combining the role-based security with the object-based security, or in this case, I'm showing you the folder security. A security within Vault will never give the user when combined with a role more permissions then they are actually given based on the role. So what I mean by that, I showed you an example of the document consumer. Document consumer is a read only consumer. They do not have read, write, modify. They can't do anything with the file.

If in the security I've assigned that user the modify permission, it doesn't matter. The role that they were assigned does not give them the modified permission they can't edit the file folder or

what have you inside a Vault. So in this case, the most restrictive combination between the role and the folder level security or the object-based security applies. Any questions on that? No. All right, good.

Overriding security, you do have the ability to override security. We're going to actually demonstrate this later. But if you have 2016 and earlier you probably know a little bit about overriding security, where you can just change the security based on the file differently than what you've put on the folder. And again I'm a demonstrate this later so I don't want to jump into too much detail here. But here's something that everyone really, really, must understand is denies, implicit and explicit denies.

So if you're looking at this-- and you're using this as an example-- I've given the administrators allow across the board, manager two has an allow for reading modify and have deny for delete, manager one has an allow but his modify and delete are empty. Those are the null values. We call those implicit denies. So I have not granted the managers, one group, a permission to modify a file. But I haven't really denied them either, it's an implicit denial, it's a null, and when you hit the drop down it's a blank. Yes

AUDIENCE: Why not making mandatory to specify a deny instead of a null?

IRVIN HAYES JR: So the question is, is why not make it mandatory to specify a deny instead of a null? I will actually demonstrate that to you. I will show you why. Because you can really get yourself into trouble if you hit the deny. All right, so the deny, the explicit deny is when I've actually selected deny altogether, all right. So that explicit deny takes precedence over any grants at all.

Remember, I'm doing this by group level permissions. I haven't assigned any users anything, right. So you must understand selecting a deny is very restrictive. And actually I'm going on record because it actually is really being recorded, use the explicit deny with a lot of care, all right. Because you're going to get yourself into trouble if you actually go and explicitly deny someone that permission. So actually, why don't we do this. Why don't we jump into a demo and I'll actually demonstrate the question that you asked.

All right, so I'm logged in as the administrator first off. And by the way, I do have-- I have some giveaways up here. I like to give away items. These are the good items I like to give away for good questions. You know, that was a good question, I'm give you one of these so. You lead right into my demo so I think you deserve that. That's good. That was good.

[LAUGHTER]

IRVIN HAYES JR: You get the shark, the fish, so there you go. All right, where did he go? A good question and a bad question. All right so I'm an administrator in here and I'm going to show you a simple configuration. Again, this was just set up specifically for our demo and our class today. And what I'm going to show you here is in this directory. I'm going I go to documents and-- Are there any sales people in here? Great, so let's talk about it. Sales people are very nosy. They like to sell things that don't work yet. So sales people, we generally like to get a model or keep the model of a designs folder, right. So if you look in here I have not given permission to the sales team to my designs folder.

AUDIENCE: You can't give them both?

IRVIN HAYES JR: You can do that too. You can not give them both. But you know, but then you deny me the selling you a license. So I don't want to do that. Now, sales people are only going to be allowed to get into the details or the documents folder in this case. So with that, I'm going to look at the security. And you can see I haven't added to the security access control lists or ACL. So what kind of permission have I given the sales people?

AUDIENCE: Null.

IRVIN HAYES JR: A null or a implicit deny. So very good. All right. So what we're going to do is we're actually going to grant the sales group permissions. This is the only folder that I'm going to allow them to come into for now. All right, so sales is in there. So I'm going start this one up. Sam is my sales guy. Let's see what Sam's can see.

So as we look in here Sam so far has access to just the documents folder that I've given him permissions to. I haven't set up the other folders. But you can see, as an administrator, I get two more folders. Sam can only see the documents folder underneath, m1. Now Sam, at this point, he can do whatever he wants to do with it. So I can take a file or a file in here and have Sam check it in. I'm good to go. Right.

So what if I had this particular folder and I said, all right well, not everyone in sales should have this permission? So I'm actually going to deny everyone else that's in the sales group. And I'm going to take Sam and put him back in here individually. And I'm going to give Sam the permission. So now I'm going to take a look at Sam again. I'm going to do a refresh. And what have I done? Because of the denies, Sam is now denied access to modify and delete of

the file within the folder. Why was he denied access?

AUDIENCE: Most restrictive.

IRVIN HAYES JR: Most restrictive and deny takes precedence over everything else. I denied the group. Sam as part of that group. He gets the denied. I don't care if I add him or do anything else. Answers your question, right? That's why you want to use the explicit deny very carefully. You can get yourself into a really bad spot. So at this point I can go back here. My intention was I'm not going to give everybody in sales the read and modify. If I remove this I have not explicitly denied the sales group. But I haven't actually granted them the permission. I'm going to come back in here and look at Sam. Now he's back to being able to modify a file. OK. So that's the real understanding that you have to have when you start using object-based security at this particular level, all right.

So we're going to jump back-- any questions on what I shown you so far? Because we're going dive further in. All right. Let me switch back over. So let's jump into a state-based security. So if you're not familiar with states, your life cycles, have various different states where are you can modify and customize them. We have life cycles out of the box, flexible, simple. There is item life cycles. I think there is a folder lifecycle and things of that nature.

But when you actually are looking at the lifecycle definition each of the states can have their own security for the object that you're taking through that lifecycle. The security options by default coming out of the box, you have two, combine and you have an object-based security. Each of the states again can have their own security but I'm going to demonstrate to you later how you set those states and how they actually start to work with the object-based security that we showed before.

For those of you who are upgrading you currently have lifecycle. You currently are using an old security model that we have. But when you migrate to 2017 are we're going to do is we're going to take your current life cycles and we're actually going to take them and put them in an override object-based security. This gives you the same security model that you had in 2016 when you upgrade to 2017.

We don't want to change those underneath the covers and not tell you about, right. So you'll keep using that until you're ready to convert over. If you're ready to convert over you can always use the combined with object-based security setting. Any new lifecycle states that you

create will have the combined option selected by default. Yes?

AUDIENCE: Is that an automatic thing or is that something we have to do [INAUDIBLE]?

IRVIN HAYES JR: Oh, so the question is, is it automatic by the upgrade or do you have to do it manually? It is automatic. So we will automatically take your current life cycles and set this option for you to the override setting. OK, but then later on we can switch it over. Within the life cycle when you go to the security tab you have these three different options, no state-based security, basically what that is saying is that when I take an object-based and I put it within that particular state it's not going to have security on it.

And what happens with that file is it stays an object-based security settings that you set on the folder. You have this other option here, which is not new, but you should understand. So the one for items, security for associated files of items, I can configure those items or those files based on an items lifecycle. And then the security will take the state of the-- or the security of the item lifecycle itself.

And this one's a new one, security for the files inside of folders. So when you take a folder through a lifecycle change and you set up the security for each of the states, the files within that folder, as long as they're not on their own lifecycle, will follow the lifecycle of the folder and its security. What do I mean by items? Inside of Vault-- inside of Vault professional there's a section for items. And they usually handle your building materials and things of that nature. Those go through there when you actually create an item. You understand that, OK.

All right. So all these security settings when they get pushed down to the files that get pushed down to the state-based security on the file. Now remember you have object-based security and then you have state-based security. But these settings get pushed down into the state-based security on the file. Any questions before I jump into the demo? All right.

So let's jump into the demo here. All right, so I'm going to first start off with-- I don't need Sam anymore, Sam the sales guy. And I'm going to show you our life cycles are set and configured. And we're going to look at a demonstration of one. So inside the behaviors have, life cycles. For this class I created one called classify.

So within the classify life cycle I'm going to go ahead and just hit edit on it. What you see-- again, this is out of the box, so when I created it the first thing it did was it chose combined with object-based security model. That's the new model. I'm going to leave it there, because

we're going to work on that later with a further demonstration.

Each of the states themselves-- So I'm showing you work in progress. If I select the security tab, what you'll see is that the administrator at this point has only read permissions. And those users that are in the group of classify have allowed for everything. So I'm trying to secure a folder to just people who have say high level clearance. So they're only going to be the ones in this classified section. So each of the security states have their own security.

So for review, everybody's read-only, for release their read-only. Notice that the everyone group is missing or not in this list. So I have-- I have implicitly denied everyone else in other groups. Now the other thing you should note here is I said security for files inside of the folder. Now this additional dialog that pops up when you hit configure has three options, apply folder-state security to its files, apply custom security to files inside of the folder, or clear the security override from the files inside of the folder.

So the first one, what it's saying is basically the lifecycle or the security set on that particular state is what's going to get applied to the file. If for some odd reason I may want the folder to have a different security setting versus the files in the folder to have a different security setting when I go to release, I can actually select the second option to say apply a custom security to the files inside of the folder. And then I can actually set that in here. So your folder and release state will have one security setting. The files within the folder, all of the folders in release state will have a different security setting.

But it is based on the state that I've just configure for release in this case. And then the clear security override-- I haven't demonstrated security override. I will still demonstrate that later on. But basically, if you've overwritten security on an object-based, or a file in this case, within that folder this state will clear that override. And it actually then goes back to the object-based security settings that you have for the folder.

So I'm going to take this. I'm a leave this at apply folder state security for the files and just hit Cancel. And let's take something through a lifecycle state change here. So with my classified folder, as you can see, the administrator showing has read only. So in this case I really got to actually log in as a user who has classified permission. Whoops. And that is Chris. Chris is sitting right here. Chris is not allowed any place else.

So inside here Chris has permissions. As you can see, if I select the upper level folder, I can see what state the subfolder is in. So the classified subfolder currently is in an work progress

state. So let's take a look at its security settings and details. Oops. Over here. Oh, you know what, Chris can't see that. Chris is not an admin. So I have to go back to the administrator.

So for the administrator you can see Chris has classified. He's in the classified group. He's allowed to do everything. Administrators are only allowed to read. That is not common, usually the administrator at least has the allow modify and delete. But what you do notice is that this says this is the state-based security on the folder. If I wanted to see what the object-based security on the folder is I can click that box or check that drop down. And you can see what the object-based security for the folder shows. And it shows the administrator has allow, allow, allow, right. But if you look at state-based he doesn't, all right. I'll explain that later so hold on to-- I see some curious questions.

On the particular file within that, if you go into details, go in the security, you can see the state-based security for that matches the state of the folder. If you select the object-based security see the object-based security also matches the state of the folder. But I'm going to take this through a life cycle. I got to take you through a life cycle for Chris-- or under Chris. I'm going to change the state for the folder. I'm going to release it. Hit OK. I'll go back as an administrator to take a look. If I look at classified security now every one has only read only permissions. If I look at the particular file you can see that the file now from the state only has read only permissions. So in this case I'm controlling the security of the files within the folder by changing the state of the folder itself. I don't have to change the state of all the files.

There are multiple rules that still apply within here, such as-- one thing you have to understand is that within life cycles you have the ability to transition or set security on transition states. So I may only allow certain groups to transfer this transitional file, or in this case a folder from work in progress to released. If I denied, let's say everyone in classified from doing that, Chris will not be able to go in and select the folder or the file within that folder and say change state.

So the new security model honors the state-based or the object-based security on the files within the particular folder. So if I don't have modify permission at the folder level I can't change the state on that particular file within the folder. Does that makes sense? OK. Let me show you actually the one thing I didn't show you were that set so that you understand. So if you go into a Vault settings it's going to lifecycle again, take a look at classified. And I'm going to go into security--

ANIL Transitions.

CHINTAMANENI:

IRVIN HAYES JR: Transitions, thank you. We're going to transition from work in progress to release. And if I go into security and I uncheck this, this is the text that you'll get. OK.

ANIL CHINTAMANENI: So in previously in Vault it's the transition security that would allow the user to perform this transition. So in addition to transition security, user must have a modify permission at the folder level to make a change state operation.

IRVIN HAYES JR: Yep, this is part of the new security model change. All right, any questions so far? So far we're good, all right.

AUDIENCE: In order for the transitions, it has to [INAUDIBLE].

IRVIN HAYES JR: I'm sorry, say that again, please.

AUDIENCE: In order to change the state from work in review to release, that modify folder usage.

IRVIN HAYES JR: So the question is, to change the state from in review to release they have to have modify permissions? Yes they have to have modify permissions in order to do that. Because what you're doing at the folder level when you say that I have modify permissions, that means I can modify the contents of the folder. If I don't have that modify permission at the folder level I can't modify the contents. Changing the state of a file within that folder is actually modifying the contents within the folder and I don't have a modify permission.

AUDIENCE: Doesn't that defeat the purpose of locking this on for review?

IRVIN HAYES JR: Not if-- so in this case-- So the question is, doesn't that defeat the purpose of locking the file in review. So in this example I'm not trying to solve that particular problem because what I'm doing is-- this example really shows you a user who's not using folder or file level security state life cycles. I'm only using it at the folder level, which means that once the folder goes in review everything underneath that gets locked down anyway. And I'm not doing individual file life cycles. I'm just doing it right at the folder level. I'm going to lock the entire folder down at one time. So that's what this example shows. We'll show something similar later. OK. Any other questions? OK. So I've either last you all are you all are getting this. I'm going to take the latter.

All right, so let's look at combine security now. I showed you a bunch of illustrations before of

life cycles security, object-based security. But now you have to understand how do they work together. So when they work together we call it working as a gated security. The first thing you have to do when you actually are working in this model you have to understand can I get by in the permission with a role that I have? Do I have enough permissions in the role?

So if I'm a document consumer I only have a read only. If I need to edit a file I can't get by the gate of the role permission to do any modifications. So let's just say for instance in this example, I'm a document editor. So I can edit files. So I've gotten past the role. The role says I can modify files. The next gate you come to is the object-based security gate. Does the object-based be security on the object I'm looking at allow me to modify the file? If it does, then the next gate I come to is the state-based security gate. Can I get past this gate and modify the object? As long as I get past all three gates I can-- I'm allowed at that point to do the permission that has been configured in this example to modify permission.

If I cannot get past one of those gates at any step along the way I'm immediately denied. So that sales guy is really ticked off when he's at your desk saying, hey, what's up give me some permissions here, right. Begging for his life. And this is one way of illustrating this and understanding it. But this is another way. So we talked about 2016 and how 2016 works. When you come in from-- or when you upgrade from 2016 to 2017 We're looking at the override permissions at the top. So this section here.

So it does have a data it permission setting or thought process. The first thing I have to get past is the role based permission. Can I get past that gate? Yes. And then I only have to check to find out if I have object-based security or state-based security, one or the other. That allows me to get in that permission. Once that happens I'm in and I'm allowed to modify the object again in this example.

If I've configured it or switched it over to this combined security model it goes back to the gates which I just illustrated. So once I can get through all the gates and both ACLs or all ACLs allow me to do this then I'm in this section here, which allows me to do whatever it is the permission that is set for it. Does that make sense? OK. Is everybody on-- for those who are in 2016 is this easily understandable for the new model?

OK. So with that, I'm giving you a chart to make sure you understand that the allow permission-- showing you in a chart-- allow at any state or may allow me but at the end if I have a deny, whether it be implicit or explicit, I'm going to get a deny. So that's what this

particular chart is showing you. Allow, allow I'm allowed and deny obviously in all three.

This one is a deny, allow, and deny. The asterisk means that if I'm using the override I'll actually be allowed. OK, this is a change. And then the rest of these are pretty much the same. And this is where you're at the group level. Groups allowed, group A is allowed, group B is allowed. If I am in both groups then I'm allowed. If I'm not in both groups I probably get an implicit deny in one state or the other, I am denied. Goes back to the upper charts. Any questions? All right.

So let's demonstrate it. Let's see what we got here. All right, so I've also developed another life cycle illustrated here for you. And I call it the engineering flexible life cycle. So I just took a life cycle that we already had, copied it, and made some modifications just for this demonstration purposes. So engineering has all the states that it had before. I do have certain security within the states.

And what I've done here is I've set everyone to allow so everyone's allowed to read in the work in progress state. But the engineers are the only ones besides the administrator that are allowed to do all the permissions. They can read modify and delete modify. The administrators can do that as well. So that's work in progress. Release, I just switched everyone to allow and only the administrators can do a little extra in the release state.

What I'm going to do is I'm going to take a look at this designs folder. Now this gives you-- when I talk about flexibility within the new model it's very flexible in the sense that I don't have to have multiple life cycles to do multiple types of security settings per folder or project. And a lot of you probably work in projects where you start at a folder level, you know M1 is one project, M3 is another project, Q5 is another project.

But for each of these previously if I had different users involved in those projects and they had to have different security settings I had to create multiple life cycles for all those different security settings. Now I don't have to do that. My goal here is to use one engineering lifecycle for the entire Vault. But each of my folders are actually going to have its own security that gives me additional security settings for that particular folder.

So within that, designs, if I look at the folder itself and I look at it's security settings, notice I split my engineering group into two different engineering groups, engineering one and engineering two. Engineering one has allow for everything. Engineering two only has the allow for reading. Managers are allowed all of them. Managers don't need this, right. Who needs

managers are overhead. What? I'm sorry?

AUDIENCE: It might as well be sales.

IRVIN HAYES JR: Might as well be sales. Well you know you said that. I didn't say that. All right, so with that I have a folder and a file in here, and I've already set the lifecycle on a particular file. The lifecycle of the files is a work in progress. And as you can see, it's got back to engineers having allow and administrators having allows as well, everyone else is read.

What I'm going to do on this side is I'm going to log in is one of my engineers. This engineer's name is Ed. And Ed's going to take a look at this particular folder. Ed;s looking at the designs folder. He's allowed to do anything he wants to. I come in here, I can check this file out. I can change the life cycles. I can do everything I need to do as Ed. I'm going to launch another client here. Erin is another engineer. But Erin works in Europe. Erin is not on this project. But the question is, how many licenses do I have? That's a very good-- I like that question. I'm sorry, I've got to give her that one. That's pretty nice. Here you go.

AUDIENCE: Unlimited.

IRVIN HAYES JR: Did you just say unlimited? He gets another shark.

AUDIENCE: [INAUDIBLE].

IRVIN HAYES JR: Well, that's me.

AUDIENCE: Yeah, I know. But how many licences do you have?

IRVIN HAYES JR: I have unlimited. I'm using one license. I may have three clients up. I'm using one license. OK. If you want more about licensing Anil and I did a class earlier today that talked about licensing, how it works and what's different in 2017. But I'm only using one license in this whole demonstration with three clients. So Erin's not on this project. But if I look into the folder, notice the first thing I see is Erin has a lock on the designs folder. If I go in here and I take a look at the file, Erin also has a lock on the file. Erin is an engineering group two. So she can't do anything. She can't modify. Because if you remember the permissions, engineering two the object-based security level was only allowed the read permission.

Let's switch this around. Let's take a look at N3 designs. And in this case, what I've done is I switched it around. Engineering group two has the allow. Engineering group one has only the

read. So if I look at the differences here, I go into that one designs, Erin has permissions there. If I go and look at Ed and I look at that one, Ed is now read only.

But I'm using one lifecycle. And I've just set up my security for a difference between the two groups or their location. So again, the optimization here is one life cycle, I can set up groups by their purpose. What is their function within the organization? Maybe it's by their location, maybe it's by whether they are classified or not classified. Do they have some type of security level for government work or something like that? Right. So I can use these life cycles and take everything in the system through one lifecycle modify my folder security, and I can have different security settings on all the objects within those folders. So any questions on that? Yes?

AUDIENCE: You have [INAUDIBLE].

There's one [? shard ?] that's coming up For one year I had to send in reports to our manager. [INAUDIBLE].

What we would do is after I shed it all, like-- would I have to go folder by folder [INAUDIBLE]?

IRVIN HAYES JR: All right, so to repeat the question. He is-- I'm going to change the phrasing a little bit but I think is what you're saying. You have to report out all the users and what access level that they have within either a project or within the entire Vault. And you need to report out on that. What's the easiest mechanism to do that? I don't have one. I have not-- we have not created a tool. Actually, Doug still has one tool. It's very outdated.

ANIL CHINTAMANENI: Yes, it's not caught up with the changes that we made with the product. So while--

IRVIN HAYES JR: He's looking to report and do a report on him. Go ahead.

ANIL CHINTAMANENI: While Doug's tool is useful, It's not caught up with all the changes that we made recently to 2017.

IRVIN HAYES JR: You know what, I do have something for you. I got something for you. It is-- are you in my class on Thursday, dashboard smashwords?

AUDIENCE: I'll be there.

IRVIN HAYES JR: Reporting?

AUDIENCE: Yeah.

IRVIN HAYES JR: Come to class. I do have-- see I do have something up my sleeve for you. Dashboard-- that class on Thursday talks about how to do advanced reporting of Vault. And I bet you can solve that problem with that. OK. Yes?

AUDIENCE: So if I understand, you are color-coding [INAUDIBLE].

IRVIN HAYES JR: So the question is, based on the-- I'm going to say the category. The categories is what's set in the color of the upper folders.

AUDIENCE: Yeah. [INAUDIBLE].

IRVIN HAYES JR: For Q5?

AUDIENCE: Yeah.

IRVIN HAYES JR: So, OK. All right. So his question is, how is the-- what's the precedence of these? What's happening is, without getting-- I am going to answer some parts of this later. But the point here is what's the security settings here? Security settings for M1 right now is only set at the object-based security. I have in a category but the category has no life cycles. So it's only using object-based security at that particular level.

But as you go down and drill down because of the combinations, like classified, I actually created a security setting for it. But if you look at it's object-based security, it was set for administrators classified. So I changed it from the upper folder. It doesn't have the same permissions as the upper folder. But if you look at-- let's take a look at Q5. It's settings security. It says that the object-based security everyone at administrators and if you look at the sub folders within that it's going to have the same. But I'll talk about-- I think I'm going answer your question better later on. OK. Yes, Jim?

JIM: To answer his question, we have to do the same thing. We report out every time-- [INAUDIBLE].

IRVIN HAYES JR: You have to--

JIM: For IP. So, an automated tool is fantastic because it would save you that extra step. Right now they have the user involved in what their permission are, [INAUDIBLE].

IRVIN HAYES JR: I've solved that problem. You've got to come to my class on Thursday. You got to buy me a beer after that class.

JIM: I'll buy you two.

IRVIN HAYES JR: You'll buy me two? Not the free ones in the event, Jim.

[LAUGHTER]

IRVIN HAYES JR: I knew exactly where you were going. All right. Any other questions? All right, so we covered that. So I wanted to give this example here. What if you had outside contractors? You know the flexibility of a security model can be used anywhere. You know I may have-- I know some people in different industries allow their contractors to come in via VPN connectivity or Vault.

But they are only working on certain contracts. I could figure in this manner where I as the manager-- Mike manager can see everything. Contractor one only has certain access to the project. Contractor two has his own access to a project. That's based on object-based security of the folders starting. And then the life cycles definition that I created for engineering could still be used across all of them. One Lifecycle definition, multiple uses, multiple security options. All right.

So one way of looking at security and how it's affecting your users is what we're going to talk about effective access. You've done all the security settings. Sam's come to you again, sales guy, saying why can't I access something? Well, it's kind of hard for you to see because security can be configured in multiple different locations, whether it's the life cycle, whether it's on the file, so on and so forth. How do you see that?

In 2017 we've added this tab called effective access. The effective access tab you can add users and see what access that user has on the object that you're looking at. We've only allowed you to add the users to this particular tab because adding groups really doesn't help you find out what that user's access level is. So right now we're only allowing you to add users to this particular tab.

As you can see, in this particular example, Mike has allow everything. Michelle has allowed,

deny, deny. Now the deny, deny shown here it can be an implicit deny or an explicit deny. But the point is to show you they're being denied somewhere. OK. But you want to end up testing these changes. The key thing with the test, which I'll take you through so you can see it. You're allowed to adjust some of the settings, see what happens before actually implementing the setting.

So let me show you what that looks like. All right, we're going to work in this folder that I have been messing around with here. Haven't messed around with yet. So within the designs folder here I have security settings for everyone. And I'm going to start adding users to this one in particular. I'm going to add at the object-based security level-- actually I need to show you this. At the object-based security level I have engineering one, engineering two. I remember Ed and Erin are my engineers.

So I need to know actually are they getting the access they need based off of object-based security and state-based security. So I'm going to come in here to the effective permissions. I'm going to add Ed. I'm going to add Erin. I'll just add Sam just for the fun of it. And hit OK. So Ed has allow everything. Erin has deny in two of those. Sam has deny all across the board. Where are my denies? If you don't know, where my denies coming from Erin?

So with this drop down here I can first take a look at what's object-based security settings. Is it object-based security? That is the first gate. She couldn't get past it. She's been denied, right there at the first gate. Well, what if she was allowed at the first gate? I can go here and hit the state-based. You can see at the state-based she's actually allowed. Why is she allowed at the state-based? Somebody--

AUDIENCE: Because everyone is.

IRVIN HAYES JR: Because everyone is allowed, right. So that's where she is allowed. But her effective access is still deny because she couldn't get through the first gate. She couldn't get through the object-based security. Now what if I wanted to test around and mess around with this a little bit? Erin is in a unique situation. I need her to modify something because Ed is out of the way. So what I'm going to do is I'm going to come in here I'm going to look at the object-based security. I'm going to add Erin, as an example.

And I'm going to say, Erin I'm going to now allow you to do these things. I may go back to effective security and now Erin is allowed. Where is she allowed? Well I can go back to object-

based security, Erin is allowed there. And I also know that she is allowed here at the state-based security. I have not applied the settings though. The settings are not applied until I hit the OK button.

So if I hit cancel and I go back into the security settings, he goes back to the way I had it before at the object-based security level. So I could start messing around with security if someone said, hey, I can't gain access. I can mess around with the object-based security to change the access at that particular time. Does that makes sense? Yes, Chris?

CHRIS: I actually had a question. Are the effective permissions for the implicit deny [INAUDIBLE]?

IRVIN HAYES JR: So the question was, on the effective access tab will an implicit deny show up as blank or will it show up as deny? The answer is that is it will show deny. Erin is never explicitly denied anything. But it shows up as a deny. That way it's-- we made it blatantly obvious that she can't get that--

ANIL CHINTAMANENI: Because that's the effective permission--

IRVIN HAYES JR: That's the effective permission she's denied.

ANIL CHINTAMANENI: And know that the effective access tab is read only the tab. And Irvin was showing you that any changes that you need to make you have to go back to the security tab. Yep.

AUDIENCE: You [INAUDIBLE]. You wanted to see the individuals, you still had to go find [? that. ?] Why didn't they recognize based on the groups?

IRVIN HAYES JR: Well I imagine that you had--

AUDIENCE: Can you repeat the question?

IRVIN HAYES JR: I'm sorry. So the question was, When I added Erin and Ed to this list, why didn't it automatically find them based on the groups that I had in the permissions in the object-based and the life cycle based permissions? Right. I had to go and find those two particular people. When we designed this we thought about that very question. We thought why not just add all the users automatically.

The challenge we had with that was the fact that-- I'm only showing you a very simple setup, right. Engineering group one, engineering group two only have a few people. Imagine if you

are working in an environment where you have a couple of hundred people in each of these groups. My performance of populating that would be tremendous. Because really all you need is one user from each group to understand the access. You don't need all those users. So just grab one user from each of the groups and you have an understanding of the effective access for those users. Good an answer. Do I get the last gift? Any other questions?

AUDIENCE: It was 700--

IRVIN HAYES JR: It was 700, what?

[LAUGHTER]

Oh, OK. All right, so that's effective access. Any questions here? Other questions? OK. All right. So now that we talked about the effective access, let's go switch back over and move a little further ahead. And let's talk about overriding security. So you've gone three life cycle states. You understand the security there. We've talked about object-based security and you understand that it starts from the file.

But what if I had a file in a state. I didn't want to change the entire folder. I didn't want to change the life cycle security because, in the example I used, Erin just needed special permissions. She may only need a special permissions on one file. I just want to modify that one file, give her the right permissions, or modify and delete permissions on that file. So that she can edit the one file. I don't have to change everything. I do this by an override on the object.

With an override, in understanding actually the security model, you've got to understand that the security model now looking at it differently is in two layers. You have the lower layer, which is your object-based security. You have an upper layer where the state-based security resides or an override resides. So we're going to do an override.

And when we do that override it's going to happen in this layer, the upper layer. It's very important for you to understand that. Because we actually remove the state-based, or we actually could copy the state-based security settings. And then you're overriding. So we're overriding that upper layer at that point. When you override again, this lower layer-- and remember the two combinations that we talked about, the combined security and the overridden security. I've changed the security for this and so now the override is what is my security-- my effective security for that particular file. Jim?

JIM: I do that on [INAUDIBLE]. Every person is going to be out in three weeks. I gotta have someone in our work folder [INAUDIBLE]. Right now, if I do the server on it, I'd never [INAUDIBLE].

IRVIN HAYES JR: All right, so his question is, can you put this on a timer. For my example Erin only needs it for a specific period of time. And I want it to automatically switch back when she's done. Can we have it automatically switch back? The answer is no. There isn't a timer. However, you don't actually have to switch it back. You can wait until it goes into the next state. The override has gotten rid of it on the next state because of the state-based security for that next state. Then we'll wipe out that override and set it.

AUDIENCE: Now, if that file were to switch back for some reason [INAUDIBLE].

IRVIN HAYES JR: So the question is, if you switch that file back to the previous state where she had the override. No, we do not restore it. We don't store the override that you've done. And it just goes back to the next security set on that state. So she won't have it back. OK. The key thing about selecting an override-- remember I showed you in the security tab you have a couple of drop downs here.

In the security mode you have the object-based security, you have a state-based security mode. I can actually select which one of those security modes, check the box for override. And what the override will do is it will copy all the security settings that were in that mode and let that be your override mode. So you don't have to actually start adding people back. If you didn't want to or you can just-- basically it's a copy of the mode that you started from. And then again the override now resides in that upper layer. OK.

AUDIENCE: Let me just ask-- the state-based or manual?

IRVIN HAYES JR: So the question is, down here why does it say state-based or manual down here? So what this particular setting is telling you is that the security settings that you've checked is an override. And that override could have been from a state-based override if you configured your life cycle to override the security. So we don't know where you've done the override from. Did you manually do it or did your life cycle say I want to override the security? So we give you that option. It was an override from some place we don't record where it was. But it is an override from either state-based setting or you manually overridden it.

ANIL As we already showed on the previous slide, both overrides are either state-based or manual.

CHINTAMANENI: They stay on the same layer, which is the upper layer that he talked about earlier.

AUDIENCE: Can you multi-select files for override?

IRVIN HAYES JR: Question is, can you multi-select files for override? No you cannot. We don't show you the security tab in that case. We haven't figured that one out yet.

AUDIENCE: [INAUDIBLE] you're not storing the override, so-- that gives you the override permission to send it to Nevada. Come back a year later, [INAUDIBLE] you forgot to give her the permission. How are you going to notice if somebody gave her that permission on purpose?

IRVIN HAYES JR: So the question is, since we don't-- we don't store the-- Yeah, we don't store how you got the override, that's correct. We know we-- but we have stored it as an override. We do know it is an override. OK. That is stored. Who did it, we don't know or if it's life cycle somebody did it manually. But you could still report on it. That it is sitting in an override state and here are your security permissions based on the reporting and how you do the reporting. Now there was another question. Mark?

AUDIENCE: So I understand correctly, you can set up a folder, which I-- [INAUDIBLE]. And can I put in a file which has override [INAUDIBLE]?

IRVIN HAYES JR: So your question is, if you have a folder, which has no ACLs and you put a file in that folder. And then you override the security of that file. So you're asking me what the effective permissions of that file is? You can't do it at check in unless you're doing it on a life cycle state. But if it's in there and you're doing the override, well you're going to start from a null no users in the access control list. You can then put in things, users or groups, at that point and set their permissions. And that override is what's now the effect permission for that file.

So if you, for instance, hid the file, maybe I can see it, sales guy can see all of the files within that folder because you didn't have any security on the folder. But that one particular file you selected and said he can't see this one, you can do an override on that one file and that one file he'll never see until you switch it. Does that makes sense? Does that answer your question?

AUDIENCE: No.

IRVIN HAYES JR: No.

AUDIENCE: By default, this should be like, cannot see any [INAUDIBLE].

IRVIN HAYES JR: OK. So he doesn't have read-- oh I see, you're going in reverse.

AUDIENCE: The file, which is in the folder--

IRVIN HAYES JR: OK.

AUDIENCE: --you're allowed to read.

IRVIN HAYES JR: I see, all right. So his scenario is saying that the sales group doesn't even have read permission. So in the example I showed earlier, the sales group couldn't even see the folder. But I want him to see one file within the folder. So your answer is that when you do that override the only way for him to get to that file is by a search because he can't see the folder. So he can not browse to it.

AUDIENCE: [INAUDIBLE].

IRVIN HAYES JR: He can find it in a search because you've overridden it's security. Jim?

JIM: Can I override a whole folder?

IRVIN HAYES JR: Can you override a whole folder? You're jumping ahead. Well, actually you know what, no, no you're not jumping ahead. I'm sorry. Can you override an entire folder? No.

JIM: You said you can multi-select to the [INAUDIBLE].

IRVIN HAYES JR: Right, so his scenario is he wants a user to have temporary access. He wants to do an override. I would say actually override is not your best bet.

JIM: So I would need to put them in a group temporarily.

IRVIN HAYES JR: Either put them in the group temporarily and take them back out, or you add that user-- if you set up the way I had it set up here in this case Erin, I can just add her into the object-based security. And because she's allowed through the object-based security, the first gate, if she's in the engineering group that already has allow for everything she is then allowed everything in that scenario. But if not you'll have to put them in a group that has it. Yeah, we had to get rid of a lot of them [INAUDIBLE]. That's what we're doing now.

IRVIN HAYES JR: Yeah, right. Yeah. So hopefully if you switch over to the combined security maybe that'll make

that work a little easier for you. Yes?

JIM: I understand you have some in quality, some in engineering.

IRVIN HAYES JR: Some in quality, some in engineering.

JIM: And that quality guy [INAUDIBLE].

IRVIN HAYES JR: Yes, temporarily.

JIM: You're saying, [INAUDIBLE].

IRVIN HAYES JR: He's-- so Jim is using-- ah-- So-- so your question is, he has them in quality, he has a user in quality-- well he has a quality group. He has an engineering group. He has a guy in quality that needs to do engineering work. Do you add him to the engineering group? You would. Or you can just add that one individual to the files that they need. But if they need multiple files you're going to have to do it multiple times on each individual file. There isn't a massive change. Right. So if you need to do what you're looking to do you're going to have to add-- the easiest way to add that person into an engineering group.

JIM: He can't be in both.

IRVIN HAYES JR: He can be in both. Why can't he-- why not?

JIM: Wouldn't quality override--

IRVIN HAYES JR: Wouldn't quality override-- what would override-- what would prevent that user from the quality group. And I'm asking you guys if it was-- if he was explicitly denied. So that's why you don't use the explicit deny. So if you add them to the engineering group and the engineering group already has all the allows, the quality group only has the allow set for the read, and the modify and delete he the null value, the implicit, he's not allowed because he's going through that first gate of engineering and through to the objects. Jim?

JIM: If I give you override to the assembly, does it do the parts?

IRVIN HAYES JR: Question is, if I give you override to the assembly does he get the override of the parts? No we don't transverse down. That's a future step. Slowdown, Jim. We'll get there. That has been requested. We haven't done that yet. We've had other users-- actually I think it was Martin that did that. Were you asking for that?

JIM: No, No.

IRVIN HAYES JR: Somebody else is asking that.

[LAUGHTER]

AUDIENCE: Is it on the idea station?

IRVIN HAYES JR: It is on the audio station I believe. Yeah so that is another request.

AUDIENCE: If I'm upgrading 2016 to 2017 and I have my override automatically done, is there is explicit denies in that are going to affect me when I start putting in the other security?

IRVIN HAYES JR: So the question is, he's upgrading from 2016 to 2017 your life cycle security has explicit denies in it, will that affect your change to the combined security? The answer is yes. So you are going to have to go in and evaluate do they actually need to be explicitly denied. I would say nine times out of 10 you don't really need the explicit deny. Use it very sparingly and heavy-- you have them all over, is that what you said?

AUDIENCE: We got rid of them all.

IRVIN HAYES JR: You got rid of them all. Yeah they just wreak havoc and--

AUDIENCE: We had a third party come and help us set it up and they put in all that explicit denies.

IRVIN HAYES JR: They did? Did you fire them? You used them for awhile and then they're gone. Give them my business card. He wouldn't do that. You would do that. Any questions? All right, so you talked about them both.

Now the next part that we're talking about is propagation. Propagation starts from a folder when you're changing the object-based security on a folder, the lower layer or low level. It does not affect the upper layer or upper level because the upper level is the state-based security. We don't propagate the states down in this case when you change it at the folder level.

So you got three options here. You're going to do not propagate the change of the folders, you go-- of the changes to the subfolder through child, propagate only that changes or propagate the entire permissions. So we can replace them all if you changed them all. And it's going

again down to the sub folders at the lower layer, the object-based security layer. We're not touching the state-based security. So that's how that works, the propagations. So we'll go through a propagation demo here. Any questions on this?

All right. So let's walk through it. Walk through a couple of things here. All right. So we're going to look at this Q5 folder. As you can see, the Q5 is actually not in a state but we're just going to work from the object-based security here. object-based security, I'm going to ahead and add engineers to it. Because in this case I just want all the engineers. It's fine. I'm going to hit allow. And then I'm going to hit OK. And there's my pop up, which says, what do you want to do? Do you want to propagate these things?

Maybe I only want to propagate the changes. What if I changed the sub level folder that has different permissions than the upper folder of this parent folder? So you probably only want to do the changes only. So I'm not going to change everything on your subfolder just for you. I'll only add the change that you made at this particular level. That's what that middle option is for. All right. So I'm going to go ahead and propagate the change. Look at the designs folder. And the designs folder you see has state-based security settings on it and nothing changed here. Why? Because we only change at the lower layer, the object-based security. And the engineering group was now added. OK, it wasn't there before, right.

AUDIENCE: When-- when you change this, and files are checked out, the ones which are influencing the [? loops? ?]

IRVIN HAYES JR: So the question is, what happens when you make this change, you propagate it through, what happens to the files that are checked out? So the files that are checked out the user still has them checked out. If you've denied it you're probably going to-- you could get into a situation where you're denying a check in and they already have it checked out. Yes, you could get into that situation.

That's a very good example. So you have to do these changes very carefully and understand what changes you're actually making. So, Yeah. Yeah, so what you might want to do is come in here, set the change, go into the effective access, and add a couple of users to see what their access change would be for the users that are already there before you apply the change. That's why we put the effective access in there. Good question.

JIM: Use your best call.

IRVIN HAYES JR: Use your-- who said that?

JIM: I did.

IRVIN HAYES JR: I'm not getting you anything for that. That was a give me. Yes if you do not-- how many of you have a test Vault? Awesome, for those of you that didn't raise your hand, talk to any of these guys with a test Vault. You must have a test Vault when you're changing stuff. You don't do it in the live production Vault. All right, so that is propagation.

Let's talk about the override. So looking at this particular folder, I'm looking at the designs folder that's in here. Now I've shown you that if I select object-based security-- and maybe I want these particular settings or these ACLs left in it. I'm going to hit the check box and it's going to leave the ACLs in there. So now I can modify these ACLs as an override. Or what if I didn't want that one? I'm going leave it at state-based. I may hit the override it'll stay at the state-based settings. I can then make my changes.

And then override and permissions are now my effective access. So the key thing here is, if you look at object-based security, you can see that the sales team isn't in here. I'm going to go back to the override. Let's add Sam. I'll add sales just for grins here. I'll give sales allow. And let's find out what his effective permission is. And it so happens to be Sam. Sam is now allowed. Why is Sam allowed? He gets through both gates. Which gates is he getting through?

AUDIENCE: [INAUDIBLE].

IRVIN HAYES JR: Is that correct? No, he actually didn't get through object-based. object-based he's sitting at denied. He got through state-based or the override. You're no longer working in a combined situation. You've overridden in all security the override. It becomes your effective permission, whatever you set for the override. OK. Any questions here override and propagation? All right, with that let's switch back.

So let's summarize. What you've now done is-- and you can go back to your offices. You have successfully understood how to configure your object-based security, how to configure your state-based security. You understand now how they work in combination with each other, how overrides work, how you can use the effective access tab to understand the security setting changes. And how all the things are affected when you actually go in here start creating your life cycles and state security themselves.

Now, I didn't again go into life cycles themselves as a whole. There are other classes that

we've taught previously at AUs. Some how I flapped that in order. You have behaviors 101, 201, and 301. I taught 301 last year. That actually talks about life cycles in depth and how you create your life cycles. It has example files in there too on how to start off with your life cycles in Visio. And then understand what you want to do with each state. And then you can go in and actually create those life cycles and security.

If you want to understand where you're at now, for those of you who are not on 2017, this rock paper scissors class about Vault security is the precursor to this one. But it's about the old security model. It gives you in depth-- just like this on-- how to understand 2016 and earlier security models. So if you really want to understand that first before-- while not before now-- if you really want to understand that, see this class. And you've already got the understanding of this class. So you're the perfect understanding administrators of Vault security. Any questions? Any other questions I haven't answered?

AUDIENCE: So do we still have access to last year's classes?

IRVIN HAYES JR: So the question is, do we still have access to last year's classes? Yes, you actually do. Even if you didn't attend AU. All the AU you material some point in time after AU is open to everyone with an Autodesk ID. You can sign in and again.

What? There's four or five years worth of Autodesk classes up there. Yeah, absolutely. Yeah, it's a great resource for a lot of stuff. Actually, I went and visited Gabriel here at Toyota and when I left-- Yeah, I'm going to throw you under the bus. When I left I sent them an email with about 20 different links to previous classes from different years of AU that I taught. Anil taught a couple of our support people up here.

Actually not-- these are new guys. They didn't teach any of them. But there's a bunch of material up there. Yeah they're newbies to AU. All right, so that's in the class. Please make sure you fill out your surveys for this class. I appreciate all your feedback for Anil and myself. And if you have any doubts of what to check it's number five at the end. All right, so just do that for me.

If you need any other questions or have any other questions after today I will be at the answer bar tomorrow during the morning and actually I'll be full time at the answer bar starting at 2:00. I believe from 2:00 to 3:00. So if you had-- if you'd come up with other questions, please feel free to come and see me. It automatically switched, sorry. I don't know how it did that.

But we also have a blog, which I write it and several other people write it. It's Under the Hood. It's a good resource for additional Vault material as well as Fusion Life Cycle material. If you have any ideas-- Jim mentioned earlier about the idea station-- myself, as one of the product managers, we look at the idea station quite a bit. Future releases you'll see a lot of your ideas being implemented. We did implement some in 2017. We're going to continue implementing them. And they're all based off your feedback. So make sure you go up there and visit the idea station. This is PLM TV, which is now, I think, should be switched over to Fusion Life Cycle. But that's it. And have a good time. And thank you, very much for attending.