Good morning. I am not sure, I am close enough. I am Jim Dray from NIST. I am one of the people that has been actively involved in development of the Government Smart Card Interoperability Specification for the last, which have been guys five years I guess. _____ and also I have been closely involved in 873 and FIPS 201. We are going to have two sessions this morning that all be leading or moderating and speaking on. The first one is about what we call PIV1. So PIV phase 1 as defined in FIPS 201, now better Jim?

Great!

And I will just be moderating that session, then the next session I will be giving about a half hour presentation on the special publications that are associated with FIPS 201, in particular special pub 873, which is essentially the technical details of the smart card application for PIV. So, having said that I will turn it over to Kayton Metta who is going to be giving the first presentation on behalf of NIST on PIV1.

Hi! My name is Kayton Metta. It is great to be here and we have been working on FIPS 201 for last few months, six months at least. It has been an exciting project. A lot of things have happened since last six months and we went through number of federations on FIPS 201. We started with preliminary draft. We shared that with public and also came up with the draft and then finally lot of changes came about in FIPS 201. My goal today is to talk about PIV1. What did we really end up with PIV1? as opposed to PIV2, because lot of times what we do is we mix both PIV1 and PIV2 together and feel that this is a very daunting task. So, hopefully, after my presentation, we can at least set aside, what we need to do now versus what we need to plan for in the future. By the way, I am taking place for Donna Dossan. She would like to have to be the one to do this presentation, but she is not available today. So, I work for _____ Hamilton and I have been working on site at NIST helping out with the FIPS 201. What I want to cover today is what does it really mean? You have to comply to control objectives. What does that really mean? I will be talking about specific technologies, I will be talking about specific processes, do we have to change things the way they are, probably, do you have to do it right away and we will see, you know, you have to come up with a plan and look at you know really what PIV 1 is asking for. PIV 1 initially had role-based process in it and after getting comments from public, we decided that it will become part of appendix A. So now, what you have in FIPS 201 is role-based system for meeting your identity proofing and registration requirements and there is a system based model also available. So what we have done is we have moved those two appendix A, which is now an informative solution that agencies may use it if they liked to, but they can deviate from that if they want or if they need to. So I will discuss little bit more about role based and system based, but those are really not the requirements, so I just want to highlight that those are in appendix A, it is an informative section. And then, I want to talk about once we know what it means in terms of PIV 1?, how do we move forward?, what do we need to do? in next six months. With that let us go into what does it mean?, what does PIV 1 mean?

I am not going to repeat the control objectives. I think, everybody knows what the control objectives are? They are probably engraved by now in your mind, but what I did want to highlight and I wanted to make it little bit different and not repetitive from what you have heard yesterday. So what I am highlighting is what PIV 1 does not specify? It does not say anywhere the PIV 1 that you have to have a card or it does not even define what an identity credential should be? It does not say that you have to implement any particular process for your identity proofing, identity _____. We have taken out all this technology requirements. There are no requirements for biometrics in PIV 1, but you do need to do certain things to get your NACI done. That does know biometrics, but in a different way. And then more importantly it does not require agencies to just go and integrate everything right now. You know, you have, you probably have physical access system guys that do physical access control, access to resources and then logical access people do something different. They are also responsible for issuing identity credentials and they probably mange the access controls within their environment and the way currently I think, the way things are now most of the agencies have something in place. And PIV 1 does not specify exactly how you have meet the control objectives? We do have to meet them, but how you meet them is really up to the agencies and their implementations. And so, what you have to do in next six months is look at what you currently have and make a case for how you meet the control objectives of PIV 1.

I have heard questions yesterday and what if I issue a card that is not even resistant to counterfeiting. Okay well, You know, you could do some other things, you can come up with something really need that does not really quite depend on the card anymore and may be have a bacon system, that is stronger that controls the access without depending on the card too much. May be a real time system that blocks people from coming in immediately rather than you know, few days after you find out that the person is terminated, employment is terminated, so there are I think, creative ways to come out with a patch or a solution to meet PIV 1 requirements, to self certify for agencies to say that you will meet control objectives of PIV 1.

In essence that is what really I think, it means to the agencies that you do not have to go, buy the smart cards right now. You do not have to change things right away. I think, what it saying is you meet the control objectives, like Bob Donaldson said yesterday. If you are making a change to your system, if you are thinking about reissuing all the cards, then, of course, you should definitely go to smart cards, but you know, before you make that change, you know, look at what PIV 1 really is requiring you? It is not requiring a whole lot and try to use what you currently have to meet the control objectives of your system.

Now let me get into little bit of what a role based system is? I brought this up because I wanted to explain what are the basic needs? And then how you meet them, is really going to be different for different agencies. Role based system basically like, I have got badges from different agencies and I have pretty much gone through a very similar process for multiple agencies. It just little bit different from agency to agency, but primarily you have an applicant who is a person, who needs an identity card or a badge or identity credentials for logging on to a network. Then you have a sponsor within an agency who decides that this person should receive the credentials and then you have a registrar. We define registrar as an entity who is responsible to make sure that you are background checks are done, that you are an appropriate person to receive the badge and you are a qualified person to receive the badge, for example, the requirement may be you are a US citizen, and so they verify. So registrar is the person who makes approval of your application and the sponsor is the person who wants you to receive the credentials so that you can either start working or start supporting them. And then the issuer is a different entity that issues either the cards or the credentials and they are all depends on what applications you need access to but there are multiple issuers within an agency.

Now that we are talking about logical and physical both. So that is the role based system where you have different people have the roles, they play the roles of identity proofing and registration. As soon as we have different roles and we have different offices and all these office roles depend on each other, you get separation of duties.

It is one of the things that you require to have from PIV 1, you get separation of duties in each role then has their particular requirements that they have to meet to make sure that they have done the _____ to make sure that they have looked at the I9 forms, at least two of them. So their _____ of requirements that you probably already have, it is kind of engraved in your mind, but if not we can go over them again and also we can get it from FIPS 201. So each one of these entities they have requirements that they have to meet and they depend on each other and at the end of the day before the issuer issues the card, he would have all this paperwork or electronic information available before they can issue the card. That is the role based system. Now the system-based model is very similar in terms of meeting requirements. The difference is that now you can have a system that manages the entire steps or the whole process of identity proofing, _____ and registration. So in this case you have people on roles interacting with system and moving an applicant through the whole process of application to getting the card or issuing the card or issuing the credentials. Similar to what you have in roles based system, you need someone who is responsible for sponsoring you. You still need someone who is checking _____ and getting your beckon information done. You still have someone who is collecting your demographic information at the initial stages and then also verifying your identity using I9 documents. Those people are there, but actually it is the system that people do not interact with each other, but it is the system that manages the entire step that you have gone through. That is kind of a system model, I don't think there is too much difference between what we have in appendix A1 and A2. What I have done is, I have taken what we have in appendix 2 as a system-based model and then I have applied the roles that I have defined in section A1. So what you see in red, the sponsor, under 3 there is a registrar, and under enrollment there is a registrar. What I have done is, I have kind of lined up the roles that we have in section A1 with what actually roles are played in section A2. Overall, this is really what you need to do, a person comes in, you ask them for the I9 documents, you validate them, the sponsor sends this information over to the registrar. The registrar does the verification of the information received, decides whether the person is approved or not approved to receive the credentials, then you go to the issuer, the issuer receives this information from both the sponsor and the registrar before they issue the card or the credentials to you. That is basically how identity management system works and what we currently have is this. There is a big mess of a lot of different redundant activities going on within an agency. Let me change this, this is not a mess it is just that everybody works in their own, small, closed environment, and it works for them. So this is what you currently have. You probably have multiple administrators in your agency administering different resources within agency and then applicant as an individual would probably need to go to all these different administrators and go through the same process every time to get the credentials and to get access to the resources that they need. I have worked with several different agencies and I have personally gone through this process where I have gotten my badge from a security office in one place, then I have to go to a network guy to give me access to the network, then I have to depend on local network person to give me access to the PC that I have in the building. There are three, four or five different people that you have to go through to get access to the resources that you really need to get you started and currently that is really the situation. You have different resources doing the same things, but doing the same things for different resources, so this is what it really looks like, this is where we want everybody to move and this is what I think PIV in the FIPS 201 will force all of us to move in a particular direction. Now, what this is, is a new way of looking at identity management. You could have a one time process where the person goes in and you collect all the demographic information you need about that person and that information once is collected, it is shared within an agency, so that you could use that over and over to give that person access to different applications or different resources and it is centralized within an agency. I just made sure that I said within an agency because distributed, centralized, we are not talking about throughout federal government, I think we are talking about centralization within an agency. So you have demographic information collected in one place, then you could have credentialing done in one place, where a scenario would be a smart card is issued to you that has PKI certificates on that to get useful logical access that has _____ or some other unique identifier that you use to gain access to a building, so you have a kind of aggregating everything in one place and issuing a credential that works across multiple applications. That is really where we need to be going, then there is authentication, authorization processes. Authentication is done using the credentials that are issued to you and then authorization is obviously determined by the application provider, if they want to give you access to their application. This is really the model that we want to move forward to, but I don't think that this is a requirement of PIV 1 and this is something that will probably take little time to get everything together and there is a lot of planning involved in this process. Lets go to the next slide, so in order to move to a unified, coherent identity management system, it is not just technology. Technology is only 20% of what you have to do or may be less. It is all about people, it is all about, you know, your business case, you need to make sure that you meet the requirements of your agency, also you meet the requirements of federal government, you also have regulations and policy requirements that are implied or that you have to comply to. Then you have people in different groups doing different things, this is kind of have to bring them all together, so you have a lot of work that is outside technology. You have to find the money to get the work done, you have the find the resources to get the work done, and that's really what I really wanted to highlight here. Identity management planning is really what we are getting into. I guess, what is also important is, you will find out that we are talking about smart cards a lot, but next six months, it's not really about smart cards, it's really about coming up with a plan. It's about knowing what your agency currently has, how does your agency function, and what are the identity requirements of your agencies, what are the credentials, what do they look like, is it user ID and password, is it pin and magnetic stripe card, is it fingerprint access to your networks, it could be many different things and you have to talk to many different people within your agency to see what it is that you currently have and lets go to the next slide. This is what I came up with as plan in moving forward, what is it that you need to do next six months. First of all you need to figure out where are the gaps, that is very important. You need to know what is currently being implemented in your agencies. You may not have a logical access application and then that probably means that you have to do a lot of work, but at least you know you have to identify it and then have a plan to get that work done. You have to figure out where are the gaps. Once you have figured them out, then you need to figure out, okay, where is the funding coming from, then what are the changes that you have to make, what are your offerings for implementing new architecture.

How would you pursue new architecture? Whether you would issue a smart card right away and start planning to make changes or would you wait until you have a PIV2 solution that you could use before making changes to your system. So between now and next six months, you have to comply to PIV1 objectives and then you have to figure out and self accurate that yourself and figure out or make a case for yourself of how do you currently meet the requirements. Again the important thing is that you may have a physical excess guys they do one thing and logical excess people they do something different and nowhere in PIV1 I see that you have to combine them now. You can take individual applications and apply control objectives to each one of them and decide whether your system currently complies with the control objectives. If it does not, you may come up with a quick patch that does not have huge implications on your implementation and then plan moving forward for a smart card issuance or not smart card issuance, but PIV2. Another caution that I guess if you buy a product now, you need to be careful if you buy one right now to be sure that it is really PIV2 when you are looking forward to PIV2. This is in case if you are buying something now. People may say that you have FIPS to one complain product, but you have to be sure that it meets a control objectives of PIV1 and we are not doing two steps, so you buy something now for PIV1 and then buy something else for PIV2. That is probably not a good idea. So you might want to look at the control objectives, apply them to your systems and see how you meet them and make a case for that and submit that to OMB as your plan and then also come up with a migration plan to PIV2. In essence, this is what I wanted to say today. This is not too much to say about PIV1. It is basically complying to control objectives. It does not even tell you what you have to do or how you do it. Is it separate within your agencies, different officers in your agencies do different things, so it may be, and it is likely the case today. But I think what OMB is looking for is a migration plan, a path moving forward to aggregate everything in one place and how do you plan to do that?

I will take questions, probably now or later. I guess, we will go through all the presentations and then will take questions. Next will be **_____,** he is from OPM, I am sorry, don't know much about him, but he will talk about NACI.

Good morning.

My name is Mark Pattro. This is loud enough.

I work as a program analyst with the Center for Federal Investigative Services, basically just across the stress from here to OPM headquarters. The OPM Investigation Service has an official roll in this entire process. We have participated in discussions on it. I have been asked for advice and will be provided from time to time when it has been asked for and we will continue to do so, because although we have got no official roll in it, what we do is a part of it and that of course is the background investigation element although. How many folks here, just like quick show of hands or from your agencies personal security, shops, not quite even half? I want to go over because a lot of the questions deal with NACs, NACIs, what are these things. I want to go very briefly and to find the terms of what we are talking about here. As was mentioned yesterday, executive order 10450 did create, what we now call the NACI Investigation, National Agency Checks with inquiries as being the minimum for entrance on duty of any federal employee. The NAC itself is not a standard on investigation, it is a component of that. As it is also a component of any higher level investigation that we would conduct all the way up to the single scope background investigation for top secrete clearance. The components of NAC are defined by executive order 12968 and the investigation standards that were promulgated as a result of that. The mandatory elements of the NAC include a check of OPMs, Security/Suitability Investigations Index, which I mentioned yesterday, check of the defense departments counterpart to that, technical check of the FBIs fingerprints, submitting fingerprints to have those run by the bureau and also the Federal Bureau of Investigations Investigated Index, which is a name check, not a fingerprint check and the cause of delay is currently in completion of these NAC is almost universally, the FBI name check because the fingerprint checks, the bureau promises us I think with its 48-hour turnaround from when we get them for the agencies and submit them and I you submit them hard card, we do scan them, so that they go through bureau electronically. They have given TS 48 hours then normally giving them back to us in less than 10. So that is a very very quick process. The FBI name check what that is, it is a check of all other investigative files, counter intelligence, criminal, background investigations, files, things of that sort. Many many individual names pop up in these files for reasons that are nothing to do with potentially derogatory or prejudicial information, but the problem is, when we are checking names like John Smith or other names, which we know that there are lot of people out there that bear them, where going to get hit and once a hit is done then the bureau has to go, in some cases manual researching through some of these files that their field officers in addition the headquarters and but say it is John Smith and we are going to couple of hits. Well we don't know if it is right John Smith and I should say we and the bureau don't know if it is the right John Smith and even if it is the correct John Smith, we have no idea at least the outside of whether or not this is any derogatory information or perhaps they were interviewed as a witness in investigation, something like that. So the FBI name check is problematic in that it takes a longtime to do and even that their end result, we don't know that were getting information that is useful to us at all. As was said yesterday, this is a resource problem for the bureau and we have been working with them to the extent of weekend and I believe the Defense Security Service has also provided some human resources to that, but this is going to be a resource problem that they are dealing with now and trying to resolve. But at the present time, it is not checked that delay is the completion of the formal NAC. Several months, many months in some case, if it is a no record if it is particularly odd name, like McMahon. It will be very quick turnaround and will have the results in a couple of days, but that is not normally the case. The NACI builds on that, it provides everything in the NAC plus mailed letters and courier, vouchers as we call them, to place it to our people listed by the subject, employers, references, neighbors, schools, things of that sort, local law enforcement agencies, covering basically the last five years of the persons life and those inquiries as was also mentioned yesterday were relined upon the good faith of the individuals that receive them. They are under no obligation whatsoever to return them. We do have a fairly high response rate. We were fearful at one point that it was a quite low, but is actually fairly high, but we can control the timing _____ returned everything, which is I think the reason why the folks who planned all this has said well it will be sufficient for the competition of the NAC portion of it in order to grand the PIV card and of course any other upper level investigations beyond the NACI or public trust investigations and/or national security investigations also all do include this NAC element. So whatever investigations are being requested now on your employees and your contractors, those are still going to be requested. If you got some one who needs TS access and this was a point of confusion early on, don't request the NACI right for the issuance of this card and then when that that is do not request the SSBI. Just get the SSBI or whatever other investigation you need because the NACs portion of that and you can issue the card based upon the favorable competition of the NAC. The issue of that FBI name check though, this is going to be initially to be decided by the _____ team leader working on, this is to whether or not the NAC can be considered complete for the purpose of issuing a card without that. I don't know what they are going to decide eventually on that, but that show something that we cannot change that the bureau was working the change, but has not been able to change yet, the time delay on that. For those of you here that don't come from Personal Security Shops, this process is going on right now in your agencies personal security shops. The process of requesting investigations are receiving them back and are judicating them. It is going on right now and yesterday it was mentioned that you need a partner with your HR folks and with your CIA folks and all that. Please also seek out your personal security folks because the background investigation part of this process is going to involve them deeply. I know there is a few familiar faces in the audience here that I know from personal security officers from the government, but seek us people out of your agencies, because they are the experts in terms of who is one investigation, how these things are requested from OPM, what we do and we get them back, how do you judicate it. Those are going to be very very important people to involve. Other questions that came up yesterday, there is a variety of individuals who do not require investigations under any existing law executive order, volunteers were raised yesterday. Contractors who do not need security clearances generally don't need to be investigated. There is nothing, there is no law, no executive order, and _____ have to ask them single question. OMB circular A130 does not mandate that if they do with IT systems then you have got to do an appropriate investigation on them, but generally there is no requirement to investigate noncleared contract as it all. If you are in a low-risk position, as a federal employee and we are going to be working less than an aggregate of 180 days, there is no requirement to be investigated either. It is the Postal Service, I know someone is still even in Postal Service that we were talking yesterday _____. They are what I think is best described as, is it fair to say Quasi-Governmental Agency and it is a change from the way it was 30 or 40 years ago. They are not subject to the NACI as the minimum. They do something very similar, which includes all the portions of the NAC I believe, but you have other agencies out there in their Quasi status that also don't fall under the NACI requirements. Military folks just coming into the service that they don't need a security clearance if they are just entering. They don't receive the NACI either. So there is also groups of people that do not now require investigations or my require investigations of a less scope than a NACI and the question was asked what we do about that and the honest answer that I have to provide to you is that the authors of this document are _____and from what they said yesterday are still deviating or discussing, who exactly needs this card. Short term people, the gardeners, things like that. There is still lot up in the air. Ultimately, it is not going to be for the investigation service or anyone at OPM to say yeah. Now you have got to investigate these contractors, you never done before. _____change in the CFR and executive order we can't do that. If however becomes the requirement, as I believe that is now for all full time, permanent, at least contractors to have such an identification. Then the instructions from this group are going to have to carry the day and if that is what this group and the final publication of the HSPD says then that is what the investigations are going to have to be and there is a resource implication. Many agencies with high volumes of contract employees either don't investigate them now, because they not require to do so or only conduct minimal investigations on them, because they are free to basically set their own guidelines for them. They do not do the NAC investigations. Many of them are only doing NAC right now or perhaps they just do fingerprint checks or credit checks or something like that. Again OPM is not going to be in position to say now you got to do that, because we can't do that without the appropriate legislation or executive orders behind us. If, however, turns out that any of these individuals we have talked about, who don't fall into these need categories, do require these identity cards as part of HSPD-12, then you will have to request those investigations and from our standpoint, you know we are ready, we will conduct any investigations you give us. We have got the _____to do it. There is no problem there, but the question of whether or not these people will have to be investigated now at the NACI level to meet this requirement is going to flow from the final version of this documented and it is going to be decided there who needs these investigations. The judication also, it was talked about yesterday using the small A for those of you in the personal security field, I am using a small A judication, here in the sense determining whether or not someone gets a card or not. Based upon the results of that NAC. The judication process for those _____personal security is as said is going on right now in your personals security shops, so as you determined what process is you going to use to determine whether or not John Dow is going to get a card their. Again with work with personal security because I think the situation _____have a disconnect their, so we are the people issuing a cards look at the results of an investigations say well, yeah, there is no significant issues you are going to get the card and then have personal security come in and say no under the judicative guidelines is that I can work here. We don't want to get a guy with the card that can't work there and similar we don't want to get a guy approved for working there who the card issue was don't deem appropriate to get a card. So work very closely with the personal security folks on them.

I think I have covered everything that I had on my notepad to address you. I would like to thank the individuals, people here for asking OPM to be here, because I know that the investigations _____ even though it is I would call a small, but significant portion of this and I know lot of people have questions. I would refer you and again another thing that your personal security folks have _____ with the investigations service and the customer services group over there that we have. The have established connections, they have established people to go to. So if you are not in personal security and you develop questions or issues regarding these things and how it impacts, what you are going to be doing with regard to HSPD 12. The first point of contact should be personal security and they have as I said contacts established with the customer service group. I would offer myself up as a point of contact for my friends here from NEST or from ONB. On policy matters they are here and I can give you my cards. But the question is about who needs what investigation, and what is in an investigation. Your personal security folks have those liaisons. So please take advantage of them. That is basically all I had and I will step down.

_____ this morning. Thank you. Those of you with cell phones, PDAs, etc, we are recording, please put them on vibrators. _____ I prefer them rather than ring for the courtesy of everyone else in the room and those who will listen to this later. Thank you.

This is a panel so we will entertain questions now for the panelists. We have until 10 o'clock and it is only 20 after nine, so we may finish a little bit early, if so we will take our break early. Jim says no based on may be yesterday's experience. Okay. Before we start with questions though I would like to place one constraint on the questions. Please only ask questions about PIV1 at this point since we do have a session on PIV2 right after this. I would appreciate that. Okay?

Good morning, my name is _____. Naturally there is a PIV1 or 2 requirement, but as director told OPM the re-clarification regarding the requirement for fresh Nackeys for Feds and contractors who have no Nackeys from the past may be and/or are older than 5-year-old, to be compliant by October 2007. Has anybody looked at this _____ been any clarification regarding our requirement.

Well first as I understand it and I would defer to my colleagues up here is if you have already had an investigation regardless of what the investigation update requirements are for public trust and national security. But if there is an investigation on file with a completed Nack, Nackey or a higher level investigation, that would suffice for the issuance of the card. Isn't that accurate.

I am not sure if you have any time limits on it. If it is 10 years old, that is no good anymore.

I think if you can find it on the file, the FIBS 2/01 requires five year issuance. So after five years you would probably, I think you have to get the Nackey done again.

Okay, and that raises a very good point also with regard to the background investigations.

I am Janice _____. I am the Assistant Director of Personal Security for Treasury. I know there is no requirement to update a Nackey every five years. You are just starting a whole new process. It is putting a huge financial burden on every agency here. The first one being that the contractors must have a Nackey now and as _____ said those of us do, we do various things with our contractors who do not require access to national security right now. The Nackey at this point in time cost a $180. Most of us have absolutely no idea what our contractor base is. And now you are telling us that we have to update the Nackey every five years and all of our employees and our contractors. We casually need to rethink some of this and I think that may be some of us ought to start pushing back of just a little bit on this Nackey requirement for a contractor.

_____. Anyway I am still shocked _____ the HSPD 12 project manager for treasury. When I asked the question yesterday that I did not think I got a good answer on, and I plan on asking it somewhat differently today. Those are point made earlier at the beginning of the presentation that we have to follow the control objectives A, B, C and D and there is no order in there. At the beginning of your presentation the gentleman from NEST you indicated that this mostly about procedure, has very little to do with the card and you gave examples on how for anti counterfeiting measures you can rely on your back end systems. If you can give me an example of a dumb card that can meet the control objective of being rapidly authenticated electronically. I have a card without any electronic information on it. It is just a piece of plastic and can you tell me without going through the expensive reissuing cards or issuing cards to new employees that are coming in, how do I meet that control objective? And how do I meet that control objective not only for that particular one, but for the anti-counterfeiting and anti-tampering.

I think the operative word is resistant to fraud, resistant to counterfeit. There are security features that you can put on your cards. There are things that you could do to your back end system to improve your ability to capture fraud faster, quicker. Again the operating word really is resistance here. I mean this is really the whole reason why I brought that up. I have made this slide up, so that you can bring these questions up now to ONB because they will be the ones to decide what is acceptable, what is not, because you will be providing a plan and in that plan you will be asserting that you meet control objectives A, B, C and D. You will be specifying how and that how is where the uncertainties are and this may be the good time to ask that question that this is what I have. Is it enough or do I need to do more.

Will someone up here, could they give me _____ I would like to get an authoritative answer on the question on whether or not agencies who do not have any type of electronic capabilities on their cards must be start issuing these cards from October 2005 to meet the control objectives. Because what that is _____ we are going to be putting in systems in place to issue these cards to meet these control objectives, but they probably won't be the PIV2 cards. And so right now based on what you are telling is even though we have until 2006 _____ for our new employees and contractors, it will take me a year off our schedule.

I think this is my personal opinion that if you are going to reissue cards by October 2005 you would want to do that such that it is PIV2 compliant or in other words you do not want to go through this twice. You would try to make it such that you do this once and plan ahead for PIV2 card.

One of the things that we have just gotten from these two questions. And then we go back to yesterday, and the comments that you have not made. Where you have objections to the draft guidance and the draft things, those should go in the comments that are due than 9th of May. Okay. So there is an opportunity for folks to voice their violent objections to things to ONB. She asked for those violent objections yesterday. Don't shoot the messengers please. We are here to convey and we will go from there. Thank you. _____.

Janice Ruffin, _____ and Affairs: I just want to make sure that I am clear. The OPM database will drop off investigations that are older than 25 years old. I have employees that have been employed who had a Nackey. 25 years ago they have been continuously employed and it is my understanding that even though there is no record in OPM there is documentation in the OPF. So I can issue a badge to that individual without updating his _____.

Well we have _____ you want to take that?

Well I'll try. But I don't know if there is anything really that I can say, I mean both the points that Janice raised, the points that they (Janice and Janice - two Janices actually I guess) raised are valid. Anything short of a national security investigation which would include the Nackey and a bunch of other as well, do not require any periodic updating. So as Janice Ruffin indicated, someone starts with the government today in a low risk position, they have Nackey run and there is no obligation on the part of any agency to ever investigate them again. Certainly OPM's guidance is that might be a good idea, but agencies have restraints and their resources and whatever else and if they do update them perhaps I just wanted to do a quick credit check or something.

Certainly, OPM guy insists that might be a good idea, but agencies have restraints in their resources and whatever else and if they do update them, perhaps, they just want to do a quick credit check or something. So, you do have those individuals in the government who exist completely above ward, who never been investigated, since their initial hiring and if they have been there for 20 or 25 years you have that situation. And actually to clarify something Janice said, most investigations unless the persons stays on with the government, as an active employee or contractor, will drop from OPMs database after 16 years. The 25-year-thing is for the significant issue cases, so only a small number, probably, can be retained that long, so there is no requirement to investigate right now. If the final FIPS document does indicate that there needs to be an update of this every five years. However, they say this, and again we are talking to them and telling about our processes, that’s ultimately going to be the call of that document because we can’t say, thou shall investigate every five years without the CFR behind us or an executive order or something like that. But, if the determination _____, yes, for the purpose of this card is that NACIs older than five years are not acceptable or 10 years or whatever they want to say for, and we can provide advice anything like that, but ultimately the document is going to have to determine what is required there. Then we will do the investigations as you have given to us, but I don’t think I answered those questions _____, but that’s what I can say about that.

I am Steve Kaye, from justice, this October you have to accredit the departments and agencies, have to accredit their PIV1 processes including their systems and providers that are involved, whether they are in house or out of house. Are you are going to be providing specific guidance/ documents in terms of how the process is supposed to occur?

Yes, I think most of the later part of today, we will be talking about implementation guidance and Frick is working on that and they will be here to help out on that.

All right, it was also indicated yesterday. For those, who were not here yesterday, that there will be another special pub on self-accreditation and control processes that NIST is currently working on.

A quick question. When you say the final FIPS document, are we talking about the OMB guidance or the federal identity management handbook, as I thought the FIPS document was final.

Perhaps, I misstated and I would refer to them in terms of the technicalities.

Yea, FIPS 201 is the final document.

FIPs 201 is the final document and that is the personal identity verification for federal employees and contractors, that’s the title of that document, which is the NIST standard that was put out, and other documents that you just referred to, there is an OMB guidance coming out, that’s really a policy-related guidance and there is a handbook coming out, which is helping agencies to implement the standard that just came out.

The presidential directive was directed towards identity verification where the existing suitability regulations are directed towards determining the trustworthiness of an individual for federal employment. The FIPS requires the establishment of an Appeals process. There already are existing Appeals processes where people can contest a negative finding on their suitability evaluation. Are you suggesting that agencies create a two-tier appeal process. One to object that. Yes, I guess the only thing you would be reviewing is whether or not there are fingerprint checked out to be the person that they say they are. Can you give some guidance on it?

I am not sure if I could help you here, but I think probably, this is something I will take back and if you could leave me your number and name, I can probably get back to you on.

_____.

All the questions that are written down, that we don't get to in these sessions, as I said earlier today, we will get you the answers back, so if you have got them already written down. I don't mind you taking questions of all the panelists, but let's do it onetime, so if can get one answer and not two different answers, which confuse the issue. Okay who is next. The questions will be posted on the web site, probably not by next Monday because there are so many of them and we want to make sure we have read them properly, so that might take a little longer, but we will get them all back up. Thank you.

Janice Ruffin again. One other question. Under 5 CFR, it is true that you do not have to request a NACI for volunteers and individuals whose employments are less than 180 days, but the requirement is that you conduct some kind of a check, so what check is that going to be?

That's a great OMB question, I think. It is a policy issue really.

So, I think we just told this is the issue of the badge. Let's get down to the core of this issue. The credential for physical and logical access, if you need the routine physical and logical access, there are certain steps laid down in the FIPS that you must go through. They did not say only for volunteers, not for volunteers, it is said if you are going to issue this badge with this credential. I said at the beginning of the session yesterday that at the end of the session there probably will be more questions than there are answers, but we would have more specific questions, so you may be not getting the answers you will want. So at the beginning of the session, I said we have an interagency advice report coming up on the 13th and part of the working groups will be to ask for participation, so we could get the policy questions at least addressed to the right people, so that we can get the answers we all want to hear.

_____.

Yes, the answer is we do need policies and procedures that do exactly what you have just said. Because the two questions in the back at room, well, what I just heard was if someone under 180 days, I mean, I would have to go through this, but then again why would you issue them?

Can you say for me the section in the FIPS that mandates the NACI be updated every five years?

I think section 5.

The question was just asked again. Let me remind you that the presentations will also be posted on the web site along with the tape of the proceedings and the questions. Next.

There is one here...

My name is David Seltzer. I am a contractor at the Nuclear Regulatory Commission. My question is coming out of several of these questions. Are we headed towards possibly at two-tier badging system for all these other people, volunteers. Yesterday, we were talking about foreign nationals that are working in the US outside and a lot of things were said, well, these are policy questions. My question is, if some agencies begin to issue PIV badges based on a lower level of proofing or some other criteria, wouldn't that then undercut the entire PIV trust model?

I will try and answer that. We have thought about this a lot and initially when he started the issuance process, we had several different levels of issuers, and then we had several different levels of application providers. I think, as we thought more about it, we realize that it has become very complex. So, in order to establish a chain of trust, I think, what we have done is require minimum set of credentials and require NACI and all these other things in the identity proofing process. To establish the trust, the card that you are looking that, the card that you are using in your system has gone through this rigorous process of issuing a card to the correct individual. We start with that and now we go to the part where you want to use this card. It is up to the application provider or the resource provider to decide what level of rigor do they want to gone through before they allow this person or authorize this individual to access the resources.

So, the chain of trust really starts with issuing and we are trying to address the intent with FIPS 201 is to try and create a level field for all the issuers. So that the card that goes to different agencies can be trusted the same way. So I do not think, that there is multi-tier card system out there _____ or a requirement as such but again the agencies may have to decide what they want and do with temporary visitor badges as apposed to issuing a long term badge to the employees or contractors.

_____ I just want to ask for clarification it is not a challenge to FIPS 201. There is lot of confusion relative to the _____ and the card. It is my understanding that you specified a five year validity period for the PIV2 card and that you have to have a valid _____ in order to get it issued. You are not in that dark man state and that you need a five year reinvestigation for the _____. Is that not correct?

I think that is correct.

Okay the other question is we talked about short term and long term. This is a long-term requirement for those that are consider long term contractors and employees. The agencies and departments and still responsible for formulating their own visitor short term policies, is that not correct.

I guess I would not get into long term versus short term. Its really up to the agencies to decide who they issue the badges to and under what circumstances and for what periods?

Hi, it is me again _____ I promised that they asked question about the cards once again. You had gone over the role-based model and the system-based models and you said these are only suggestions and each of the bureaus and agencies can come up with their own process. In the roles based models, there is certain characteristics, certain functions that are, yes, attributed through like a registrar, like taking the picture, taking the prints, taking copies of the _____ documents that are presented. Is there any thing in those roles that you describe in the role based model that you would consider to be mandatory for accreditation.

Can you repeat the last part please? I am sorry I missed that.

Okay. What I was looking for - Of those roles that are listed in, I guess the informations item on the roles based model. There are different things that are attributed to sponsor or through a registrar or to an issuer? Are there any of those activities that those folks are supposed to do, are there any of those mandatories for accreditation. For an example is it mandatory that we take electronic copies of driver's license that was given to us as a _____ document?

I think, it is mandatory to have I-9 documents and verification of the I-9 documents. Not verification or at least looking at it making sure that it is not a counterfeit document. There is no requirement as to who in your agency does this or what label did you give to them. That is why this information is like it is in appendix A, it is not part of main body of FIPS 201 and the roles that we have defined they are, let me just say that just roles that we came up with and it does not have to in their label. See does not have to be the same way in your agency and that is why it is an appendix, it is not in the main body of FIPS 201.

Yeah but it did say that at some point of time you are going to give us I guess guidance on your accreditation process. And I would assume that there would be things in that guidance that would tell us those things that we must do versus those things that we could do.

Yeah, I think, the guidance does not come out yet but most likely it would tract the requirements of PIV1 and then when you respond to the check list to OMP, at that point you will probably describe you know, what the house of your agency.

Jim before the next question could I just make one quick comment on I have heard a couple a sort of an undercurrent and a few of the questions regarding the relationship really identity verification to identity proofing or authentication versus access control and just to sort of help set a stage I guess. It is important to keep the two separate. It is possible have a very strong identity verification mechanism in our PIV card operating at a high level using cryptography and still not to be able access certain resources based on the decision that an agency has made. So access control and authentication are related with _____ two separate things. You can have strong authentication and still not be able to access resources. Just wanted to make that statement and we can move on.

_____ from NASA. The requirement to have back on checks and our contractors probably going to require every government contract to be modified. There is no far requirements for that, that may need, a change will have to be made _____.

I suspect than try nothing.

Steve _____ from Social Security. I think it is in the ONB implementation guidance that is what you are also commenting on that GSA is tasked with adding that to the far by October 27th 05.

Repeat is that the implementation guidance that you would commenting on says it will be in the far by October.

We _____, end of question. We _____.

Okay, real _____ on the

_____ is here. It just, we are _____ yah.

Yeah, Ran Martin form a commerce. This is in reference to the, I-9 document. Now when you read the I-9 document it says that retention of the identity proofing documentation is optional. They do not have to retain those like copies of the passport, and those types of things. Now if I am hearing it right your saying that we have to keep some type of image of that, because the I-9 document has a certification that somebody has to send an affidavit or signa an affidavit relative to seeing those documents. So now if you saying that we have to retain it that kind of makes it mandatory where the I-9 form itself. The INS forms says optional.

Yeah, I think there is a requirement that you have to maintain copy. I am not 100% sure I pretty need to go back and check FIPS201.

Okay, yeah there is a requirement in FIPS201 that you maintain copies. It does not say whether electronic or paper work to be maintained them of I-9 documents that you _____

FIPS does say you must retain.

Right the I-9 documents.

Okay the I-9 documents not a problem but the documents that you are validating you do not have to keep like the copy of the passport or copy of _____

It is fair question goes the guidance is ambiguous.

I think, I-9 documents, it could be _____ passports, ID cards, state issued ID cards, so it depends on what you have used as your I-9 document.

(Twice seeing no hands)

I am not sure it is the right time to ask this question, but as far I am waiting for Jim to go and _____. Are we all clear about what, we talked about lot about issuance. Are we all clear when we have to use the card to access control by when? I do not think the implementation guidance is clear on that that some language _____. So I want to know, what is your thought on that.

I think, that is something that to be definitely need to tack this back and make sure that is there in implementation guidance. It is just _____to all it is pretty clear that you have to use the cards once, twice, _____(Okay you have _____ to not mumble into the microphone, sir.)

Jim Sorry.

HSPD 12 is pretty clear that you have to use the cards and FIPS 201 came out with part I and part II which is PIV 1 and PIV 2 to give some extra time and room for the use of the card and I think FIPS 201 also says that you have to use the cards and then the next thing to do is I have make sure that also clear in the implementation guidance.

The question is when we have to issue cards? When we have to use? I am sorry.

We have to use the cards is that the question?

Not the issuance of the card but the use of the card in physical and logical, am I correct?

If you are asking for the dates by which you shall start using PIV cards and the dates by which your agency is supposed to have completed its FIPS 201 deployment, those types of questions those are all I would not be _____ because there are time line and policy. So others in the audience may be able to address that but NEST can not set those time lines.

And I think again let me reiterate. For there is people if they think any place in the guidance is unclear, questionable, objectionable, etc. You asked yesterday by the "Queen of the Event" _____ please get it end and then shall put together a group of folks to wrestle with it.. So we are using this forum to surface as much as we can obviously in advanced of the 9th deadline. So you guys have been real good about _____ we do not like some of this stuff. Let us go. Let us go. As I asked just on a sheet of messengers, you know, you can cause a little mental distress. That is fine they are dealing with it with that. Anymore?

If you think you have seen all the mental distress _____ next upcoming months.

Okay with that like to thank our panel and if you would give them a little big appreciation.