050504_GSA_0900_Intro_Overview_of_HSPD_12

The introduction of how we got to where we are, are the first victim today. I mean the first guest speaker today is Tim Polk of NIST who has been a gracious guy on the ____ and all of their presentation and development of the documents that we are all now trying to digest. So, with that here is Timothy.

Thank you, good morning and congratulations on making it through the various lines in getting in here this morning. I was quite, quite impressed by the turnout and by the, the number of people here already this morning. I am Tim Polk from NIST. I'm actually one of the PKI guys at Mist and was one of the members of the FIPS 201 team, put together these various documents and well, it's been, and it's been kind of an adventure. I was looking at over my slides and I was realizing that when HSPD-12 was issued, my son was starting fifth grade. He's still in the fifth grade. In that amount of time, we have completed one FIPS, two special pubs.

There is another draft pub, draft guidance. If you're having trouble digesting it all at this pace, you're not alone. It's inevitable when we work at this kind of pace. I am still trying to sort out exactly how some of the things finished up as the documents completed myself. There is a row, the second row on the right hand side and there certainly are some sprinkled seats you may want to fill in to those of you that are standing. I think I'm going to be too longwinded to stand through the whole thing, I apologize for that. The whole thing does start out, the whole driver for this is HSPD-12. This wasn't something that NIST decided it wanted to put together and then this was something that was the mandate and that we have done our very best to be responsive to and I think that you'll see the point of my presentation here is to kind of show how we have attempted to respond to all of the various pieces of the HSPD-12 and how they draw out through the FIPS and through the various special pubs and kind of give you an overview of how it turned out the way it did.

We're going to work at a very high level of abstraction in this talk and hopefully all of the details will get filled in over the next day and a half. So, the requirements, got a couples of slides here on HSPD-12's requirements, I think that this, this first set, this first slide is really some key ones. The first, the first one based on sound criteria to verify the employee's identity. Based on sound criteria, we did a lot of these, we did lot of exploring in terms of what this does really mean, how do we be responsive to these. Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation, again I can read it quickly, but we spent a longtime talking about exactly how do we respond to each of those phrases. Rapidly verified electronically and issued only by providers whose reliability has been established by an official process. We had pieces of the puzzle that we could point to from various disciplines, but we didn't have everything right, right at our fingertips to do this.

Then, those are sort of the, the major drivers and then there is a lot of other pieces that helped tie the whole puzzle together. So, what was the scope? Basically everything that's not a National Security System, that's a specific definition you know who you are, but everybody else is in the scope of this, federally controlled facilities, federally controlled computer systems, very broad scope of what we're trying to address with this because of the scope, you're going to see a lot of different things that will fall out in the design and of FIPS 201.

Flexibility - When you start to look at something that broad, you cannot have a one size fits all solution. We have done our very best to provide you with a variety of tool kits, that you can use in different ways to achieve whatever level of security is appropriate. I am a computer security guy not a physical security guy. "Security commensurate with me". It is the sort of the watchword. We have done our best to give you a set of tools that you will be able to find something that meets those requirements. Something cost effective and implemented in a manner that protects the citizens' privacy. I have given this at the tail end here is a second slide, but this was actually also a big driver and has real ramifications that sprinkle through all the documents. We tried to do a lot more than give lip service to this. We think this is extremely important and there was a lot of attention paid to this. So how do you lay all this out and have this all done on the very aggressive timelines that are in the HSPD. How do we achieve the full vision that Bob Donelson was talking about this morning of being able to use these credentials across agency boundaries to get us in the door here at GSA in a both safe secured and

efficient manner. Well there are different pieces that could be addressed perhaps at different speeds. So FIPS 201 ended up being a two-part standard. The first part is really identification and security requirements.

These are things that you should be able to implement because they are. For most agencies the biggest changes would be changes in procedure and process and as much as possible we tailored those procedures and processes to the things that you are already required to do but tied them together in a way that would give us more than we got before. As has been said earlier you have to get your HR people and your physical security people and your IT people together to make this work. On the other hand just about everything in here is something one of those groups already knows how to do. Already is required to do. By tying the pieces together we get more bang for our buck. So we tried to meet those identity-proofing requirements by establishing registration and issuance requirements that would really get us, help us meet that strong identity verification process requirement. We established the groundwork that you can meet those privacy requirements and all of that is done in part one. In part one all of this is effective October of this year, that is October 2005.

Part two, is where we tried to bring interoperability to the puzzle here. You will be able to meet part one and still not be able to get in the door in a fast and efficient manner here because they may not be able to recognize and process your credentials. Things that meet part one will meet all of the security requirements, but will provide the interoperability for us to get everything that we really want out of this process. Part two establishes interoperability requirements; it establishes a common set of credentials it is detailed technical specifications when you take it with the special pubs that support this. That when we get to the point of part two, being fully complete and fully implemented across the agencies we will be able to fully realize that vision that Bob was providing this morning. There is not a set timeline for part two. Part two is not set in FIPS 201 and that is going to come from OMD guidance. That actually has to happen. We have got the specs in place. That is the end goal. So part one is the first step in the process and meets basically the spirit of FIPS 201, but does not give us the HSPD 12, but does not give us the interoperability that we need to fully get on return of investment. Part two finishes that process. So I am going to go over the requirements both in part one and part two. First and foremost organizations have to adopt and use an approved identity proofing and registration process. We want to bring commonality to this process. Even though all agencies have very similar requirements in terms of what they are expected to do for identity proofing. The identity proofing that has been associated with badge issuance either has not been as consistent or at least has never been believed to be as consistent.

One of the things that I discovered very early in the FIPS 201 process is that every agency was happy with the way they did identity proofing before they issued badges and they were satisfied with what they thought other agencies did. So one of the first things that FIPS 201 is doing is bringing a level playing field to that. We are pointing to the requirements that already exist in OPM and saying that badges don't get issued until a NAC is completed. You already are required to have a NAC for everybody, for all of your employees. What we have done now is we have tied the OPM requirement that you already had to the badging process. Completion of the NAC though is sufficient for you to issue the badge, because the NAC can take months to complete and we understand that once you have hired people you need to be able to get them in the door, get them on to your systems and you need be able to have them be full contributors as rapidly as possible. We are also requiring that the applicant appear in person to get the credential. We do not really think this is that much of a burden when people get badges, we take photographs of them today. We can't take a photograph of someone who is not there. So we have tied once again. We are trying to tie these various processes together so that the FIPS 201 credential actually has all of those good properties. Again these are probably not things that you weren't doing before, but we have put it into the FIPS to ensure that you know that other agencies are meeting the same requirements that you are meeting. Two forms of identity source documents for the applicant for a badge. One of them has to be a government issued picture ID. This is not really an onerous requirement and it is probably what you already been doing, what you now know is that other agencies are definitely doing the same.

Separation of duties: I think this is the one that will cause some pain in your agencies is making sure that you meet this requirement. You may already have this in place, but this is something you are going to have to verify. One of the problems that we have in some places is badges. Can badges be issued by someone on their

own volition? If they just decide to go issue a badge the process should never let any one person make that happen by themselves, because if they decide to issue of fraudulent badge whether it is to their friends so that they can buy alcohol, whether it is to somebody so they can get in the door.

The important thing is that we want separation of duties so that we can ensure that multiple people have all agreed that this credential is necessary. We do not want credentials being issued by federal agencies unless there is a need for them. So that is what this is all about. I have to use an approved credential issuance and maintenance process. There are requirements about how you deal with the badge after it is issued. That is actually very important. It is one thing to make sure that a badge is issued appropriately. Its one thing to make sure that badge is issued appropriately, but what if it should have been revoked and was it. What if that information never makes it into the appropriate databases? But what if the fact that I was fired never gets sent to the people who actually maintained these databases, who would have done the revocation? If these things are all tie together, we won't get all the security we are paying for. One of the other things here is that we have said somebody in charge is now going to have to make a decision that "Yes, they have looked at how the process is being done and it is acceptable". This is actually probably always been done informally. I think something as big is your badging process or HR process, it does not just sort of happen, but what we are saying is the way if these things are tied together needs to be approved. Now, we gave this one whole slide to itself because as I said earlier, the privacy requirements were something that we really took to heart and something we tried to follow through all the way through the document. There is a lot of ways that you get to tailor these cards in your agency and you should keep these thoughts foremost in your mind as well as you are working on how to tailor these cards for your specific agency requirements.

What we have tried to do in FIPS 201 supporting documents is ensure that we have not done any thing that really compromises the privacy of the badge holders. Most of what is done in part I is really though, I am only talking about part II there and about how you implement this in your own agency. In part one what has really been done because it was called out specifically as being important in the HSPD and because we felt that it was referring to a lot of new laws and things. We really called out all of this stuff very directly in the FIBS. The need for a privacy official role, the need to conduct a privacy impact assessment, having procedures to handle IIF, and handle privacy violations, having the appeal procedures these are not new things that NIST invented. These are actually things that were already in the laws and the regulations. These are things that were already of requirement. We called them out specifically in FIBS 201 because we felt they were key to being responsive to the HSPD and we wanted to make sure that they were highlighted and given the right amount of show time there. So part II is the detailed technical specifications.

As I said at the beginning, I am a PKI guy, a crypto guy. There are an awful lot of pieces of this that are not PKI and crypto. There is an awful lot more to badges. There is an awful lot that this is much more important. I mean that is very important as well for different applications and so there were a lot of new things to me. I have to learn an awful lot. We had to bring a lot of expertise in and you know meet with a lot of different folks to get this all to come together. One of the areas that I found a kind of fascinating, although I had nothing personally to do with this, was the amount of blood that was spilled over what a badge should look like, over where the data ought to be put on the card, where the picture was, how big it should be. It is a blood bath and I understand why it is very important. It took me the first couple of times that I came to GSA headquarters here. I stood in a wrong line and I signed in as a contractor. As a non-agency person, I did not realize I could go through the employee line and nobody understood, none of the guards realize the NIST was actually a government agency. So nobody told me I could go through that and when I looked at the badge that I would show them, it looked nothing like a GSA badge. As far as they were concerned, I could have come from anywhere and who can blame them?

Every agency’s badges look very different. FIPS 201 is going to bring some commonality to this. We made everybody unhappy with the result of this, which is what we consider to be a good standards effort. That is the thing that you know everybody had to compromised, nobody got everything they wanted that is probably good. I can tell you that my badge does not look much of anything like what fixed to a FIPS badge is going to look

like either. So do not think that NIST just wrote up theirs. So, but we want to at least have a certain set of fields that are always on the badge. Those are listed as mandatory information on the left hand side. There were a lot of things that some agencies felt very strongly had to be on a badge and other agencies thought should never ever, ever be on a badge. Well, a lot of those things became optional data. So that you can meet your agency's requirements and other agencies who feel that for example the written signature is one of those, some agencies felt that having that on the badge was key, others felt was a bad idea. We have tried it, but the thing is you can count on when anyone comes from another agency to your door, you can count on all of the things on the mandatory list being on that card and being where you expect them to be. So even for the guard at the gate, doing visual identification, we hope that we have improved the interoperability of the new devices.

For this one I really would have liked to have reformatted the slide. I was looking at it last night when it was far too late to do that, but I am going to do this top bottom and then middle because the top and the bottom are really all mandatory. There were a lot of different possibilities for what things could be done, but we settled on the right answer to provide security to meet the HSPD requirements and do it with interoperability was a smart card. So, yes, it is mandatory that the PIV card as we call it, will have an integrated circuit to store and process data. Those interfaces at the bottom are also mandatory both contact and contactless. We recognize that there are applications where you need to be able to wave your card at the reader and go one through. There are also applications where that is not a requirement and that additional security mechanisms that we can do through the contact side really make sense. So we have both.

We looked at doing one or the other when we started this process and there was actually a lot of blood spilled internally at NIST over this and in the end, we came to the conclusion that both had to be there. There are the abilities to add optional things to your card. Magnetic stripes, bar codes, you know it may be that to support some kind of orderly transition at your agency, you are going to need to add bar codes to the PIV card because that is what you are doing now. We did not preclude that. We want you to do what makes sense in your agency, what lets you do an orderly migration, but that was not a mechanism that we felt was going to be responsive to the HSPD in the long term. So it is something you can do as an added function for yours. Those are the kinds of things that we have tried to do to make sure that a PIV card provides interoperable mechanisms and still lets you do the things that you need in the short time them to support an orderly migration. So we said we are going to have a chip on this that is going to be able to store and process data. So what is this data that we are going to be storing and processing? It is mandatory that the card support authentication of the user to the card using a pen. That turns out to be piece of the puzzle that we will use with numerous different controls here. So, what is this data that we are going to be storing in processing. It is mandatory that the card support, authentication of the user to the card using a pin that turns out to be a piece of the puzzle that we will use with numerous different controls of idea. There has been cardholder unique identifier.

Basically, there are a lot of components to this, but what is really important for most of us is, there is a credential number it is global across the federal Government. There is an agency code within this, it says issued by missed or issued by Department Of Defense, and that will enable us to be able to recognize, in that way we know that if NIST issues are credential number, no other agency will issue a credential with that number on it. Each agency is responsible for making sure that these credential numbers are unique, but you would know then that if you enter someone in your system from another agency that you add their credential number to something that in your access control system, you know that there won't be another agency that will issue that same credential number. It is also an expiration date within this _____??? and the expiration date you recognized that the card is actually expired even if it does have a good credential number. There is what's been called a PIV authentication data. There is one mandatory cryptographic key for this card, called the PIV authentication key. There is a certificate that goes with this and this allows us to do cryptographic authentication mechanisms, then there is also two biometric fingerprints on the card. There are a number of optional pieces as well. Three different keys that can be used by the cardholder to do really non HSPD#12 things which is why they are optional, which is digital signatures or key management, it is the key transport or key agreement, RSA key or _____??? key. We will get more about all those details later, since that what I know and so I cannot _____??? into those details. An optional asymmetric or symmetric key that can be used

without entering a pin, so that you can use that with the card reader that as a flash pass as you walk by, to support higher speed authentication and then it is optional, but I would strongly recommend that everyone support the symmetric key for card management, so that you can actually update data on the cards, so that if something changes you do not have to throw way your smart cards and get new ones. That is not really an HSPD requirement, but it is a good agency decision. As we said, the HSPD said there had to be graduated levels of security to address the different range of application requirements, and we tried to look at the fact that everything from visual identification by the guard using the badge, as I said I think we have enabled that and enhance that and improve by putting all the same information in the same places on the card. The _____??? as I said this is a credential number that can be read of the card in a very efficient fashion. We do not make you enter a pin to let that information be read by the reader. Since it is just a credential number, it really does not have a lot of privacy implications. Biometrics on the other hand if you want more confidence you can use biometrics. The biometrics that are stored on the card for _____ ones requirements require that the user enter a pin happens more slowly, provides higher confidence you really have all three parts of something you know and something you have and something you are at that point, and then those are really most useful in the physical security or sort of local authentication.

The PKI credential is one I like to think can be used in every range, of course I am a PKI guy, I would think so, but it is another mechanism that you can use and in that case, we are able to distribute using the federal PKI we are able to distribute status information. Using the federal PKI were able to distribute status information. So not only can you verify that this was a good card really issued, but you are going to be able to verify that I was not fired yesterday as well. As I said in the last few months since the HSPD was issued, we have done an awful lot, an awful lot has happened very quickly. FIPS 201 itself is the centerpiece of all of NIST efforts but it is not the only missed effort and it is not the only government effort to be responsive to the HSPD. And to get the full picture, you need to actually look at all of these or you have to look at whichever one of these other documents really impacts your personal, your place and your agency's response to the HSPD.

There are three special publications that NIST has done, that add further technical detail to the FIPS. One of the things that those of you who are familiar with FIPS process probably know, is that FIPS are very hard to change. We do not update them every year. There are not new releases. They have to be signed off on by the secretary of commerce and I have seen a number of FIBS that sat, go over, that took between the time we though we were done in the time the secretary signed it, that have taken a year. Now we managed to do the whole process this time in six months but we are not counting on ever being able to do that again. So pieces that we think may have to be changed a little more often to respond to technical change got relegated to special publications.

There are three special publications that are referenced by FIPS 201. Special publication 800-73 is actually the technical details of building the smart card that we are requiring in FIPS 201. There is 800-76 which is actually still a draft which goes through the technical details of how you format and encode the biometrics so that we can achieve interoperability. If we are not all using the same encoding we won't have the interoperability across agencies. That piece has proved a very difficult nut to crack and we are still in some flux on that one. SP 800-78 goes through the cryptographic algorithms. Most of the PKI pieces are actually in FIPS 201 but there were an awful lot of pieces that had to do with what cryptographic algorithms can you use to implement a particular function.

If we did not fully specify this information, you will not have interoperability because I will be using Diffie-Hellman and you will be expecting me to be using RSA, something along those lines. All of that information got placed in a separate publication and this is probably the driest and most boring document you will ever read but on the other hand I think it does lay the basis for interoperability. I can say that because I am one of the authors of 78. So the fact that I am bored by it is okay. It only does what it needs to do. But those are the kinds of things where if something happens in the world of cryptography, and we decided an algorithm needed to be phased out earlier, we would update this special publication. It is a lot easier to update this pub than it is the

FIPS. There are a whole lot of things on this website frequently ask questions, lots of documents, for we have a NIST website devoted to this project. I would encourage you to check out the information that is there.

As I said though NIST is not the only group that is trying to be responsive here. The HSPD has requirements for all of us and there is a couple of particular areas that I would say you need to be sure that you look at that you are familiar, because FIPS 201 is only part of the story. There is the OMB guidance. There is the thick implementation guidance and there will be more NIST documents that have not even been drafted yet on things like certification and accreditation. So it was a recap. We have come a long long way since August 27th. There are an awful lot of things that have been completed. There is an awful lot for all of us to digest. It is not all finished. We are going to learn more as we go along here. That is inevitable when you have a project that brings together the IT security, the HR and the physical security worlds, in a way that I really think has not been done before. So it is going to be a wild ride and I am glad to see everybody is so interested in getting started.

Thank you. RI???

That is your turn. Tim has been gracious enough to leave us his time. So we will start from the floor if you have any questions. Hold on I will come back to you. Thank you very much. My name is Michelle _____???. I am representing ATF. Four real quick questions.

1. Encryption key pair -- if that will be allowed on the card here -- seems to indicate excluding that. Here also you have an alternative options for the card and you did not indicate whether or not an option would be, say an HID capability, so you have dual contact lists??? and bios. Is that going to be stored on both the contact lists or just one?

Okay. Let me make sure I get each one of these. The first one is, I would expect for example that NIST implementation. We actually use an HID card right now. I would expect that it is a different mechanism for working with the contact list reader. It is actually a resonant cavity card. It has no intelligence but it chirps back when the reader chirps to it with the credential number. I would actually think that NIST for example might implement a dual contact list and contact card for its initial implementation, because that way won't have to toss all of its HID readers. I would think that over time as all the readers migrate to become fully FIPS 201 to a one compliant, that wouldn't be a requirement anymore.

The first question -- encryption key pair. This is one of those ones where it is all my fault because I chose the wording on it. But this is a really common misunderstanding. What people think of is an encryption key pair, as what we are calling the key management key. So whether it is key transport for RSA or key agreement, in general you do not want to encrypt data directly using a public key algorithm. What you do is you encrypt it with a symmetric key and then you use either key agreement or you use key transport to make sure that the receiving party at the other end is able to recover the right key to decrypt the data. We absolutely believe that that should be on the card. It is not a requirement to meet FIBS 201, so we felt that had to be optional. But I would encourage every agency to add that key and to add the digital signature key.

The third question. I lost the third question in my head. The biometrics FIPS 201 specifies that the biometric be available through the contact interface. So you have to enter a PIN for this information to be available. The reason for that is because that anything that is available on the contact side, the guy standing behind you at Starbucks with his briefcase could actually be reading the information off of your card. We had a lot of debates about whether there was a real privacy implication to having your biometric. Your fingerprint read off of there. I leave fingerprints everywhere I go. The only place where you won't find my fingerprints is on my desk and that is because it is covered with papers. But everywhere else I go I leave fingerprints. It is not clear that that is really the most important of the privacy implications, but that was the decision that FIPS 201 made. We believe that as cards evolve. We believe that as cards evolve and you can authenticate the card reader that it may be possible to move the biometric to the contact list side as well, but only when we will know who the reader is that is asking for the information before we let it go. That actually was something that we talked about, but the

infrastructure requirements to make that happen were onerous and so we went with the contact side, it was the easiest way to make the privacy requirements be met.

Good Morning, I'm Kevin McCoy. Under PIV1, you talked about rapidly, electronically verifiable.

Could you define it a little bit more because does it sound like Smartcard? Does that basically mean that proximity cards or bar coders, mag stripe electronically verifying the card is the legitimate card to get into a building? Will that meet the requirement?

There is some debate on that. I see people saying no and other people saying yes. The wiggle room in part 1 was because we were not specifying a particular requirement. If in fact you are able to read information off of the card, verify the status, do all of this in an automated fashion, you know, I think you meet the requirement for part 1, but part 2 you are not close, but that was why we spread part 1 and part 2 to out to give you time to do that migration. So, you know, we are all doing the best we can for part 1, that is what it comes down to.

We have one more question and then I am going to ask the rest of you please, online and here, pass them to the middle as the second panel will get up. So last question comes through this gentleman. Thank you. My name is Chuck ____???. I am the HSPD12 Project Manager. I think, I have a pretty simple yes or no question. You will say _____??? earlier that in PIV 1 it is mostly going to be process and procedure that we have to satisfy. Some one said we had to satisfy the core objectives specified in section 2.1.

Now, if I have an agency or bureau that's issuing badges today that don't have any of the qualities let's say to prevent it from being counterfeited or prevent it from being tampered with, October of 2005, do I have to issue new badges? I do not think that the badges that you are describing meet the requirements. When I said, I think most of the agencies issue a badge that is more than just plastic cards stock and so that was why, well, many agencies. Okay, so may be I overstated and over simplified there. You do have to meet the core objectives, but we are not going to tell you how you have to meet those. We are much more prescriptive in part 1 with what you have to do on the process requirements and perhaps that is an important clarification. I am glad that you called me on that one. Yes.

Yes. Ladies and gentleman, Timothy. That is all that is going to get addressed until later this morning. That is really an OMB issue and OMB is here. I just see in your agenda. Thank you, thank you Timothy very much.

If we can get some thanks for Tim this morning.