Ladies and gentleman for this particular panel we are privileged and privilege is the right word to get some feedback to get some guidance to hear some words from the folks who have been at the pointy end of the sword literally at the pointyend of the sword for a number of months on this. And several folks have tried to back them up with some success but with that I would like to pass the mantle to Janelle Thornton, Judy Spencer from GSA and Curt Parker from NIST. Ladies and gentleman it is yours.

Good morning everyone how is going, I feel like a walked in to hostel territory and we can look with humor it is okay you can laugh. I really want to you all take a deep breath.

I have repeat that those of who still want to laugh. I feel like I have got in to some hostel territory here and I want that you all take deep breath. And really think about some other things that the office of management and budget understands our issues that we are working through and some things that we have tried to do in the development of standard in the guidances to make this as easy as possible for all of you. So we are in the beginning process of that and so I think there are still some questions and we need a answers to. To got a follow up on the last conversation before I talked to specific thingsI was going to talk about with regards to opium. I have taken a specific action I am going to set up senior level meeting between OPM, OMB and FBI and I will have some conversations about specifically those questions are answered. We will get back to you on of all of that. As well as seeking some input from agency HR representives and other folks who like to be involved and some of these specific questions are getting answers to them and we will through them. You know we are getting through these things I think it will be all right so I have taken a note as an action item, result of this conversation so I appreciate that. Before I get in to some of the more specific and some of the things are you like to know more about. I want to do set the contacts in terms of why the office or management budget role in all of this is has been and will be over the next few months, I think that is really important. I first is you know, I promise you that I am not going to use the word ISO and see during my remarks because I really think it is important to think about that big picture here, what really do we have to do?, What we have do by when?, What is it going to cost?, How can I procure this in a easy manner we are may be I do not need to know all the technical details, but I need to know how to write a contract _____ a got to a GSA to get what I need, okay that's really what I want to focus on here. We thought that was important to specify those sources of things in plain language not looking at lot of these technical things in implementation guidance. You know because we have a lot of effort to lot about some of other technical details we have really guidance to in the session of lot about. Some of the practical reality in the things than your want answers to, Who would my agency to does apply to, which contractors, You know, does my agency even passed the complaint you know thins like that. That I think really important to spell out in plain language in guidance so. I think most of you probably have read the draft, implementation guidance and comment period closes on May 9th so I am looking for to all of your comments and I am assuming the most of the issues you are raised today and terms of these sort of things. We will be addressed in your agencies comments so that OMB can take a good heart look at your comments are and make changes based on those. So thus are really, really important to ours in terms of what you all have to say. I will say that again, again, again that is extremely important so I am looking for to all of your comments on time of course so that we can move quickly to address some your comments and your concerns.

Some of them in the high level, I have talked about the implementation guidance our sort of role facilitate some of these high level policy issues that you heard about today and finding ways to get them addressed. So we will be working on some of these over the few months and we already have addressed many issues that agencies have brought to us with regards to specific policy questions. Those of you that are familiar with the directive understand that by June you have to have program in place and we have got no out of questions about what that means and Judy Spencer is going to talk a little bit of about that more detail. I am not looking to see your agencies line by line project plan or implementation plan I need to have some sense on behalf of LMV that you all have taken the right steps so we try to put a template it is got some changes based on all of your feedback in place it we can do that and Judy's going to talk about that. I think it is also our role at the office or management budget to try to ensure a consistent implementation across the government I think it does not make a lot sense for all of you to be tackling this issues independently as we learned. I think it is extremely useful for there to beyou know there is service opportunities standard documentation which I wil talk about when we get to the privacy presentation little bit latter. Standard documentation, other materials contracting vehicles etc that are available to all of you. Because we certainly want you do focus on those issues that are they sent to your organization and your agency and not having to be worry about some these standardized things so we can do once and not have to deal 20, 25, 30, 35 times, so I am looking for more feedback on some of those areas in terms of what those might be it was just mentioned this morning and some of the HR in the investigational requirements is one area that could be a lot more done across the government to pool our knowledge and resources and we will take care of that. I am sure you have many other issues similar to that will need to look out of the next few months. And finally I think the most important from all of your prospective malpractical side is really to ensure at oversede effect that the general service administration is going to be there to provide you with complaint products and services at the lowest possible price. I think it is a fundamental issue here frankly there are still lot work to be done over the next few week to months to make sure that happens and that sort of what is an extremely important piece that Judy talk more about that we feel is absolutely necessary for you all to be successful in implementation of this directive. Thank you,

The two things that I am we are going to focus on this morning in terms of some of the things we are going to talk about either the plan which is due in June which Judy will talk about and I am also when I get to the privacy conversation talk a little bit more about the provide the list of other applications you are familiar with. I would not go into any more detail.

You know it is kind of difficult to talk about he implementation guidance in a lot detail because it is going to change. It going to change based on your comments, so what is listed up there are the categories of information that are covered in implementation guidance right now. I have gotten several request that I am going to address sometimes of other categories for example I have got in several agencies are specifically mention records management requirement and issues related to that today I like to see addressed. And I am sure you have others you know a lot of questions this morning about specific things in the implementation guidance and frankly how I answer those of going to depend on your comments and we are going to making changes for what's, it is all part of this whole process were about to go through. I think it is very important to know who the directive applies to and you have to by when and I have gotten lot calls from agencies over the past few weeks with the very specific circumstances that apply to your specific agency that you need question to all work to those and I am getting calls form VA and other about keep a working in hospitals nurse sort of thing I think that the key here is that we want to meet the intent of the president's directive but we are not trying to go crazy here you know, what I am saying. We are try to provide a practical flexible approach to all and we all can meet the intent of the directive without going ballistic and so you see some of those things in the directive in the guidance so try address those concerns you know we are not taking about summer interns here.

You know this is one example. We are not talking about someone who just shows up for meeting at your agency you know you want have specific principles that we all use to implement this so we can really get the maximum benefit at the most reduced cost. And those of the kind of the things are recovered in the implementation guidance. And there are lot of this questions this morning about the scheduled you know, what to I have to do by when?, what is for, when is part 1 to be implemented and when is part 2 to be implement. It certainly not my intention and I can't speak on behalf of the office management budget. You develop something that you throw away in six months you know, just a meet some control objective in for one. Really talking about here is having something is done you do right now. We can take a quick at we can change how we do identity in background checking at your agency. We can ensure the contractors our part of that we can make some changes today to really improve the security of our federal facilities and federal informations systems and that the part one is getting at. Part two is really getting out.

What do we have to do to have a technical interoperable CARD management CARD governance across the Federal Government and what is I can undertake and this is kind of where the rubber meets the road, and then the guidance, we will guide you till October 2006. We know it is not possible for you to do that by this October. We acknowledge that, I think that we have tried to provide you all within flexibility in the guidance and how you implement this to give you more time to implement some of these very technical things that you have heard about today, I think that is extremely important, so we have really tried to design guidance that gives you the practical instructions that you need to apply this to your specific department in or agency. I think the acquisition services that you will hear more about, we wanted to make clear that we want you to use pre- approved products and services, so that you know when you go to vendor X that you are getting a product that is already compliant with the Government wide standard. We do not want you to have to worry about that, we want you to able to have that comfort level. We have also recommended that you use some of the aggregated purchases and things that GSI will be putting in place, but if you can better a price somewhere else, then you know that’s your product, you can do that, and we provided you with the flexibility to do that. We hope that the GSI will put something in place of that you would not be able to get a better price on your own, but you have that flexibility. I am going to talk about, when my colleagues wont be either clear men arrives about the specific privacy or requirements. I will hold off until later this morning. For those of you who have lot of employees and contractors who follow on to the National security clearance process, we have really provided some guidance in the draft guidance on that, specifically you know that someone who already has a secret or a top secret clearance, have to go through this old process, the answer is no. I mean they really are complimentary process as in which we tried to design that in the guidance, but you may have some comments in how we can improve that, and that’s fine. Is there anything else, I must consider or must no, and that sort of the catchallcategory. One of the things I was talked about in the earlier panel by the departmental stay you know, I had some really high security people in very dangerous places across the world, and how do I really insured that they are protected. There is something called as special security rescue, provision that’s understanding which provides agencies in those situations some flexibility that we certainly that want to put on your employees and contact you at risk that certainly is not the case, and still the guidance talks a little bit about that as well, let me just make sure I have got everything that is in that section, yesterday, this is something got in place serving under cover and all that. So that is our guidance, and try to make it in plain language, we do not mention too much about the part of a technical details, but sometimes becomes confusion when the technical things are tried to interpret in, we are sure we will get comments and we will make some changes based on those.

You know I heard a lot of your comments and concerns. I think this is also that we can do its important to figure out, what really is meant by success implementing this directive. I think we as a Government will not be as success as well unless general service administration plays an extremely strong role in really providing those services and providers to make it easier for all of you to implement as directive. After reducing cost making implementation easier and providing a markedly place that you can go to security services. So we are going to depend heavily on the work that Judyis doing and _____ goal to ensure that this happens for all of you when time to meet the deadlines. So it is extremely important for this. I would _____, also thought of the phasing, we have gotten into a lot of questions already this morning, and I am certainly should there is going to be more about how do I really phase in overtime, and I think that really help us to find success like I said earlier, I am not intending for all of you to do something and throw it away and then start over again, and so I think the definitions how we define success is extremely important. Also finally the collaboration peace, I think you know if honestly you have see the collaboration among the smart card community in terms of technical focus, but now its time to brighten that collaboration and put somethings in place, so we can collaborate along HR issues, privacy issues and I have already been having several meetings with the privacy committee that OMB hosts about how we can collaborate in that regard. So I think collaboration is going to be the key for success, you are all not in this alone, and we can do this if we all work together, so I think that is extremely important.

I am also looking for all of you to identify the gaps in terms of, and I think it will be important to have a conversation after these two days of sort of workshop is okay. You have told me a lot about this, but I am still not clear about this, and identify where those gaps are, and how we can provide teams to address those gaps in a short time for your questions get answered and your needs get met, so please let us know wait and welcome to give me a call, and I have spoken to many of you already about, okay you know Jeanette this really is what I needed at my agency can you really help us out here, and we will be happy to get the resources in place to provide assistance. I was just thinking about this morning as how putting this together, I think it would be helpful and has to talk to GSA about this, has been providing a resource with the sharing of ideas whether that is some sort of collaboration zone or a best service; something that we could do for all of you, who actually doing the implementation have that resource. We should talk about that, I should put them on the action list. Now what about you all, I think it is extremely important for all of you to get your senior leadership commitment to implementing this directive. You are not going to be a successful without it, and I heard Mary Dickson's speak yesterday at the _____ conference that I was added about this and I was extremely important that you are not going to be successful, unless you have the senior level commitments, I think that is the only way all of you are responsible for. I think it is also really important for you to all have the can do attitude, you know we can do this, we can protect privacy, we can address these issues over the next few months to the next year, when you have to have the power to implement, we can do this sort of, I know its feels good to complain, and to vent and all of that, but I am looking for a specific suggestions and improvements that we could make to get you what you need to be successful and I am sincere in that and those of you have known me other initial that I worked on I really I am sincere in doing that and I am addressing these questions and comments that you all have so we can get through them. I know that you have probably have way too many questions since the time allotted for me, so what I am going to do is let Judy and Kirk follow up and then we will take questions. Thank you.

Probably says GSI, IAB is on the way back from Chicago this morning, so I missed the Tim Polk presentation. Hopefully, we wont be too redundant. I am going to go very quickly through the process up to date what is in the current FIPS, and then through a list of things that we already recognized need to be done, documents we have to get out within the next month or two for your review.

These are the requirements you probably seen them quite a few times, the one thing that I think I would point out with respect to the requirements is that, one of the primary goals was to move identifying information from the visual realm to the electronic realm, and the reasons for that hardly there are some privacy advantages, but the primary reasons has to do with fraud and forgeability. We can provide cryptographic signature protection for electronic data, and we can fit that within a security infrastructure we have determined over the years that visual verification of badges provides fairly spotty level of security. My favorite case was about twenty five years ago, when a man entered a highly classified DOD facility by flashing a pack of seven cigarettes, they just happened to look a little bit like the badges that was in use at the time.

It supplements, but does not replace the guards.

Okay. We do have two parts. Part one is focussing on the identity proofing, getting that into place and getting an issuer, accreditation capability in place and under way. That is going to be a foundation for establishing mutual trust among our organizations. The second part is technical interoperability of the logical and electronic components. We are requiring conformant to part one by the end of October of this year. Part two in the OMB guidance that has come out for us to review and draft gives people until October of '06 to really get moving on that and I will get into a couple of the knack issues in a couple of minutes. With respect to migration time frames, it is not just part one to part two. But within part two, there are some organizations with very large installed bases. The Department Of Defense has something like three million cards in the field. So with respect to the electronic and logical aspects, there is also a migration from what is compliant to standards that we had in place recently and still there to the full PIV2 interoperability designed for multiple source procurement and interoperability between vendors.

Okay. How we settled on NACI was among other things we found that it was already required. Executive order 10/04/50 signed by President Eisenhower in 1953 required completion of the national agency check with written inquiries for all government employees. It also had a number of requirements with respect to personnel characteristics, so that was on the books. The material that is in the FIPS with respect to what goes into a NACI came from the office of personnel management and we examined a number of alternatives to doing the NACI The office of personnel management is, however, the organization within the government which is primarily responsible for this function and the AOP felt fairly strongly that that should be the organization taking the lead and making the rules. We do not require completion of the written inquiries before the badge is issued. The electronic component to the national agency check, the fingerprint checks, the law enforcement check through the FBI, that part is required. Depending on who you talk to, it can take anywhere from one to two days to several months. I do not know at this stage how much of that has to do with local procedures and arrangements with OPM. I do know that OPM essentially sells the background checks as a product. I also have been told that when we provide fingerprints as part of the check, that if the fingerprints are provided in electronic form, it goes very quickly. If they are provided on paper, there is a requirement to scan them in. First they go into a queue, then they are scanned into electronic form and then they are submitted electronically. So that will take quite a lot longer. We require that the person appear for the credential and this is to reduce the opportunities for fraudulent issuance. The two forms of identification are unsatisfactory and there is absolutely nothing that we were able to do about that. Some of the hijackers on 09/11 had obtained valid drivers licenses fraudulently and used them to get on the aircraft. Birth certificates come in a bewildering array of formats over the years and there is simply no way to expect someone to be able to verify the authenticity of birth certificates at least given the resources that the HR and local facility police have at their disposal. So we required verification documents and as part of the NAC we required that a form be filled out. It is generally an SF85 for most people and on that, you have to provide addresses, employment and education and all that this really does is that it gives us a chance to check on your assertions. I had been careless once or twice in the private industry and had people who turned out to have last been employed by a vacant lot. Hopefully, we can reduce the occurrence of issuance of valid credentials to people who should not have them. The background check increases the risk for someone attempting to fraudulently acquire a card. It is not proof, but it is probably the best we are going to be able to do at the moment. We looked at much more extensive background checks and of course the price of those goes way up on a per-person basis and the time that it takes to perform the checks is much longer than it is for the NACI.

Okay. We are requiring an approved PIV credential issuance and maintenance process. There were some questions from the earlier presentation having to do with well what are our guidelines for doing this approval. We should have an issuer accreditation guideline out for an expedited public comment within the month. I am expecting that we can get our first draft out in just about a month. It is being worked. We are going to focus first on the material that people need for self-accreditation, but we will also be working on third party accreditation procedures and those will be harmonized with the requirements of special publication 837, which is the driving document for certification and accreditation of systems. I said before that only the NAC needs to be completed before the cards issued. If the written inquiries come back with prejudicial information, then the agency can revoke the batch. What constitutes grounds for revocation is essentially a local matter. We are saying that the checks have to be completed. The executive order 10-4-50 says that we need to be a good moral character etc etc, but each department and agency has its own local criteria in addition to the OPM guidelines for hiring and granting access to their facilities. Philosophically, I am viewing this credential as a key. It has a number of components that can be used for access control. The design of the access control system into which the key goes and the features on the key that will be used by those access control systems are within the purview of individual departments and independent agencies.

At first this is self accreditation it is essentially analogous to information systems accreditation. There are procedures for providing certification evidence to the accreditor but accreditation is a management decision. We are hoping that the guidelines that were coming out with will give sufficient basis for making such a management decision intelligently.

Privacy requirements: Philosophically what we are trying to do is to make sure that every one for whom the credentials are issued. Knows what personal information is on the credential. How it is safeguarded and for what purposes it will be used. There is a sizable number of documents required under the privacy act that are all designed to achieve that end and those are spelled out in the OMB guidelines and they also spelled out in part I of FIPS 201 as a list. This should not be a new requirement laid on most organizations. Most human resource organizations do capture information on individuals and they should perform privacy impact assessments and identify and inform the individuals. However this is the special application, it is a new container under which to carry that information and it is backed up by additional records. So the impact assessment will need to be modified and the information in identifiable form will need to be clearly specified to each individual receiving a credential.

Okay. With respect to issuance, the primary thing that we want to achieve is the cards are issued to people for whom some management entity has requested access to federal facilities and information systems. We also want to make sure that no single individual is capable of issuing a PIV card. We had the benefit of the experience to the department of defense, which is issued something like 4.5 million CAT cards to date and they provided as with a lot of advice in a systems with respect to what we needed to do and some of the things that could go wrong. They found that the average corporal issuing CAT cards had the capability to issue cards that were incorrective fraudulent in some way to other people. The most common use of this was to issue incorrect or fraudulent cards to their friends with only one change, the date of birth. This proved very useful when you went on leave. They have made a number of changes based on their system. They have wonderfully complete and automated personal systems and basically the idea is you do not issue a card to anyone who is not in the system. Not all of us have that kind of system in our human resources area or personnel area. So we came up with two models, a role based model in which we identified a number of roles for issuance and a system based model for those whose people who have automated systems already in place in the procedures to back him up.

I am sure you have seen this card issuance and managements subsequently system. The message from this is that we specify the card, the readers, the issuing stations and the information exchange formats in FIPS 201 we are providing for the creation and issuance of a key. The access control system, the locks are left to the individual department and agencies.

A number of questions have come up regarding why we have some of this optional information on the card. A lot of it had to do with legacy, we are having to accommodate not only that information required for interoperability amongst government agencies but also to accommodate that which is already in the field in the millions and in some of those we can just by edict issue a change. In the case of the Department of Defense the common access card is negotiated through Geneva convention. They can't change it on their own. It negotiated, it is a treaty item, so we did accommodate optional information that many agencies would probably choose not to include on their cards and many agencies were dealing with labor unions and very strong privacy advocacy groups would probably be very well advised not to put on the cards.

What we have attempted to do with the card topology is to provide common look and feel. Each agency will have a slightly different set of requirements in terms of what goes on the card. We had some organizations who simply wanted the picture and name. Some weren't too sure that we needed the name, others wanted a great deal of information on the card. So what we did is come up with a layout that gives a common look, so that someone who is doing a visual inspection will be able to recognize the card as probably being a government ID card and protect from over printing several areas on the card that covered sensitive electronic components. The red area in the upper right hand corner is one such area in contactless cards we probably would not want to print up there, so we do that with that.

We do have on the card couple of numbers that are significant. One is an issuer identification number which allows tracing of cards, when an organization feels that is necessary and an agency card serial number that actually comes with the card when it is delivered to the issuing facility. Neither of those numbers is associated necessarily with the individual and certainly not in a persistent manner. You get a new card number when you get a new card and the cards will wear out. The experience with the contact cards is that they need to be replaced once every several years, there is wear and tear.

What we require is at least one integrated circuit on the card. We have contact in contactless interfaces, by the way that should say 14443 on the last line on 1443. We have some optional requirements: magstripes, bar code and two dimensional bar code. We are not saying those need to be on the card, but we are saying if they go on the card where they should go. I would like to say one thing about the contactless interface it is not an RFID interface. ISO 14443 is designed to be read at a distance of no more than a few centimeters, not like that. Some experiments were then conducted to try to increase the range with different antenna configurations to may be something like that, for going through gates or need arms so long. So far those have not worked out well. It is really a short range card.

It is possible to read it at a greater range. It doesn't have its own power supply and what that would mean is someone would need to beam power at you sufficiently strong they could probably feel it and wouldn't be good for you. The card is not designed to be used to track people around buildings.

The electronically stored data, there is one semi-persistent value on the card in electronic form. It is an employee number that is assigned by the employer and it persists with the individual as along as the individual is employed by that the employer. The other information that has to be on the card in the card holder unique identifier is generally its numeric informed and has to do with identifying the employer and the status of the individual, is the individual or government employee or contractor or foreign national. Would do require fingerprints on the card FIPS 201. There is a special publication that would provide format information for that and that's currently under review, get to that on my last slide. PKI information on the card is probably the most important mechanism going forward for identification purposes and access control systems. We have one that is required and we have a number of optional numbers accommodated.

I think Tim probably went through this but this just a iteration of what goes on the card holder unique identifier. That is the only information on a card available for free read. Free read means you don't enter your pin. For other informations that is stored on the card on the electronic form, it cannot be read out unless you have authorized with a pin or someone else who have must know your pen has done it. If you using biometrics it is difficult for them to succeed in doing that.

We have attempted to treat the whole life cycle issue from card issuance through a card termination. The thing that is probably going to be the biggest challenge for us is card termination. People tend sometimes not turn in the card in when they leave. Particularly if they leave in a pique. Capturing the card is something that we say needs to be done, but recognized cannot always be done. Again that takes back to the PKI certificate as a valuable identifier on the card because we can revolt the certificate and at least that mechanism would not work.

One of the questions was why biometrics. We are trying to provide for three-factor authentication – what you know, what you are and what you have. The card is something you have, the fingerprint is something you are. We can associate the fingerprint and the card and using the pins we can associated both with the individual. We can do the same thing of course with a visual identification which in the physical security realm, we expect will occur for the foreseeable further. If you could skip over the next one, I think, Tim that one and we will go to the last one okay. Several supporting pubs are already out there. 873 as designed to specify the interface between the system behind the reader and the information on the card. There is a provision for transition for people who have already installed large numbers of cards in the personnel base. This is necessary. Some of these people have three-year replacement schedules, in one case a very large one they just entering into one of those right now. To certainly say to them hold it we will come up with the brighter shiny interface that permits better procurement options eliminate some of the sole source and we help you with this. All you have to do is replace all the cards in the field just as soon as we figure out how to program bright and shiny cards. I suspect if this would generate resistance and would not be defendable economically, so we have transition interface which matches up reasonably close to already out there and was worked out with the interagency advised board taking there input as the driver. We have an open standard interface for the long term and expect that over the next several years every one will have same interface standard. We are trying to achieve backward interoperability to the extent that we can between the two. Biometrics there are two ways to store biometrics, one is minutia, basically if you want to picture it , finger print overlay, capture a set of points of intersection and captured whether there is a fingerprint line there and if there is what direction is that running. Using that we can come up with an order of magnitude less storage requirement on the card and much faster card reader performance. Unfortunately we do not have an interoperable capability with that right now and we are probably not going to have firm basis for that for at least a year. We do have standard that would work for fingerprint images, kind of a digital photographs of the fingerprints stored on the card. That takes it more time in processing it takes up more memory on the card and meet quite a lot of resistance from people who have practical experience in using the cards. At this stage we are waiting for policy decision from the Homeland Security Council regarding whether we go ahead with images now or wait a year and see where we are . So biometric on the initial cards is something that is little bit up the air. I am hoping that we will get reading from the homeland security council within the next week or two. Cryptographic algorythms we would put that into a special publications because the requirement change over time. Those who follow up cryptography will see that they just withdrew the digital inscription standard, its key is sufficiently short that they can be essentially the system can be broken in near real time. We worry about RSA with smaller keys. We need to be moving to 20-48 bit keys within next five years and as we start moving that direction and we start counter up memory cells that are taken and the number of keys people might want to store on the card. This says that we need to remain flexible with the respect to cryptographic guidance. We have a number of other documents we having to get out very quickly and supporting artifact. We need reference implementations. We need demonstration cards. We have to have compliance testing material including compliance test, facilities accreditation guides and accreditation procedures or compliance testing procedures. We have to adjust FIPS140-2 validation to met cards to be in the field within the necessary time frame without doing any thing that reduces the confidence that we have in the properties of the card the confidence that we have in the properties of the card so what we trying to do is to come up with a streamline method for getting validation evidenced to the CMVP program. We need demonstration prototype systems from issuer systems, reader systems, the whole suite. As I mentioned before the issuer accreditation guidelines will be out very shortly there is a preissuance guideline that needs to go out almost immediately, development guidelines as distinct from the others, for the people who were developing the cards and working how to program the cards. Development guidelines are needed for both the transition and the end architecture interfaces and there is quite lot of PKI certificate management details need to be worked out. One of the things that is not worked out in the Federal PKI, is how much a certificate costs. That’s left to the individual organizations to negotiate and some people negotiate much better than others, some have told me that they are faced with something like $40 a certificate. You multiply that times your number of employees, this may be economically more than painful. So one of the things that were hoping to work out with people like GSA assistants in our negotiation. We were putting out a graph document on the website that's up there, the OMB policy guidance is available for your review on that website and with that I would like to return it over to Judy.

Good morning everyone and I am going to be fairly brief here, I am going to tried that condense what I want to say in just of couple of minutes, but I think it is very important that we get Janet back up here to talk about the privacy piece from the OMB perspective. But to just a address of couple things that Janet said I was going to address, my master calls and so I answer, as chair the Federal identity and credentialing committee one of the things that we have been struggling is the role of FICC as we go forward, so I have actually had a meeting with some of the leadership and it is lot of the same people that are leading in the smart card space, but then also add to that the people are leading in the federal PKI space and we what we have agreed to do is we would like to morph the Federal identity and credentialing committee into that steering group that will help agencies with implementation, where we can actually work together through some of the big issues as Bob Donaldson said earlier there is a lot of experience out there but there is also lot of people that are coming to this, you know brand new, babes in arms, and we want to make sure that nobody is out there alone feeling adrift that we can actually work all this together, so that is actually what we are hoping to do with Federal identity and credentialing committee going forward and actually there is a meeting of the Federal identity and credentialing committee as soon as next week where we will talk about this and some of the plans for that group. Now in addition to that there was some mention of what GSA is going to do going forward and did you find it is got implementation. GSA is going to do going forward, so what were are trying to do is we are trying to set up, but we are calling in authentication component, which will actually be a place, if you will, a one stop shop you can go and find the products that have gone through the conformance testing and have been certified or approved as meeting the requirements of FIPS 201/HSPD 12 and we already have the first of these setup. We don’t actually have it into the authentication component yet but we do have a process in place for testing PKI service providers to ensure that they are providing service that meets the requirements of FIPS 201. Now in FIPS 201 if reference is something called, the common policy framework for federal PKI, but basically it is the policy which is the minimum requirements for deploying PKI by federal agencies to federal employees and what we have done is we have setup this thing called shared service provider program were entities can come in and qualify as meeting those requirements and provide and essentially be approved or certified as meeting the requirements of the federal government and they get to importantly they get to express the common policy object identiifiers in their certificate that they are issuing to those federal agencies. Kirk was right, currently basically you would make your own deal with those folks by virtue of schedules there will be a maximum price that they can charge and then you will be to negotiate with them under that. Another important piece that I want to bring out here because I think I will talk to you about it again tomorrow afternoon but just in case some of you are not here tomorrow. If your agency is running a PKI internally, there are agencies in this room that are. If you are running a PKI today and it is cross-certified with the federal bridge, at least medium assurance then you are compliant with the common policy. Alright, nobody is telling you today that you have to shut down your internal operations and throw out the baby. Because we have the shared service provider program. You are actually compliant, so you can to continue to issue certificates internally to your own employees. Treasury comes under that state department DOD USPTO and there are others. So if you are cross certified by the federal bridge already, you are okay, you are fine and there is in fact there wont be an OMBmemo that actually states that they came out in the January timeframe. What I really want to talk about today is that date right there and I am going to come back to this tomorrow afternoon. What I would like to do those of you there are going here for the two days. I should hear all the speakers and we have these panels. I want you think about what they are saying in the context to what you need to do. This is actually based on the control object of HSPD 12. We developed a template and actually it was Janet said earlier that this is the team effort, we want to do this together. Well you know, we are very closely with Janet and I can tell you that she agonizes over all of this and she really does want to make this as painless as possible. Tony said it was daunting. I will give you that there is going to be a little pain, but we all need to share that as much as possible, equally so that each of us feels it a little less I think. So what Janet did going into this, she said you know we need a template that the agencies can fill out and we do not want it to be difficult. We want it to be something that there won't be onerous we are not taking about you know in fact she specifically said we are not talking about 300 process. We wanted to be easier than that, and so we came out with this concept of a template and originally we said what Janet says lets make it yes/no questions, but we found out that we try to make a yes/no questions you will all be saying no and so we say said that was not quite good enough. So now what we have got is we have these approximately 20 multiple choice questions, when I say approximately because that is the count that was in the draft that went out last month for you to comment on and the final has not actually been released yet. So we are not 100% sure what is going to look like it is in the OMB clearance process and we hope it will be out soon, but you know OMB wont be too much process, but I don’t it is going to change a lot my feeling I hope not. So there is approximately 20 multiple choice questions and they range from deer in the headlights to II have to think about this or not started. All the way through I have already got that I am done and cool with that alright, and so those of the five things and as you go through the next two days I want to kind of think about where you are with the lot of the things that you folks are going to be talking about, because you are going to talking about PIV1 and PIV2 and the things that need to be put in place and so think about where you are in your agency. I think you as you do that and you should think through the actual filling out of the agency plan. You will be able to better figure out what your answer should be and tomorrow afternoon what we will do is we will work through the draft plan. We do not have the final yet, but we can work through the draft plan and actually work out, you know if got any additional questions things you do not understand about what the plan is asking you to do.

In the plan things are basically separated into five areas there is four control of objectives and if we have not beaten those things to death, yes we will have to beat them unto death by tomorrow afternoon so I won't belabor it and also the privacy piece she actually have to test the steps you have taken to absorb the privacy requirements of the FIPS 201.

Alright so think about what we were doing tomorrow we will work through this again a little bit more closely and hopefully by then a lot of your questions will have been answered but knowing these process is probably lot more will have been generated and we will go into more detail a little bit about what in the implementation guidance we will talk about that about what agencies need to be doing and how the handbook can help, because we will be talking tomorrow afternoon as well so with that I want to turn this over to Janet so that we can finish up this morning with privacy discussion.