The panel is actually going to get into some of the issues that Jeanette talked about this morning. As we were talking about the different components of physical security, HR, all the different components that it is going to take to implement if you will, HSPD 12 while a lot of people have looked at the IB as a technical working group, I actually worked for the CFO. I do not work for the CIO. In fact, we have physical security folks, might come from the physical side. We actually have embraced the HR community from the beginning. So even though a lot of people see us as the IB smart card people, we are actually the program managers with money inside the agencies to implement these things. So the people are even confused about who we are, sometimes we are confused about who we are. Any way, I have not got a chance and I would like to do it this morning. I think everyone else has been introduced. Mike could you stand up please? Mike Boller is the incoming chair and currently co-chaired at the smart card IB and I look forward in working with Mike in the transition and him taken the leadership reigns over the next couple years as we go toward these implementation strategy, but any ways thanks Mike. Again the focus this afternoon of the panel and in each, we are going to have a time for each panelist to do a little presentation, a little discussion about what they are doing to embrace all the different aspects the componentry that is going to take us to do, an HSPD12. Again prior to HSPD12, a lot of us were doing this for business or security or other reasons any ways and if you will the discovery process that we got ourselves involved with suggested that we needed to have the logical security, the physical security, and other staffs working with us as we were implementing, you cannot do it without it. I guess that is the easy answer, but embracing in a wider sense and getting more people around the table, we have already seen more people here today that is a positive direction that we headed in and even the fact that we had more privacy people involved. A lot of us have done privacy impact assessments, a lot of us has done privacy act notices and so again some of the things that we are trying to deliver across the entire government. We have done pieces parts of and some agencies are a ahead of other agencies. Collectively we might have done at all, who knows? That will be part of our discovery process. With that everybody else Tim Baldridge from NASA, Kevin Crouch from DHS, Mike Suvac from Department of State, presentations you got them all loaded? We are ready? You got one, one presentation, Mike’s. Mike, I guess you are first.

Mike - My name is Mike Butler. I run the common access card office for the Department Of Defense, for others if you do not know, we have 3.5 million cards and credentials that are out there and normally we present our, we issue about 10,000 cards a day in our department. So that is our normal like everyday workload that we provide. What I want to do here today is over the last few weeks, we have tried to take apart the requirements of the fifths and see what it means to our department. You know, these are going to be very high level, and it may be it will give a feel for even somebody who has been doing this for a number of years. There is still a lot of work to do. So these were our reference documents, the FIPS 201, the special pubs and we are still waiting up for the requirements for the Biomatrix and right now, we are trying to figure out. I mean even at the level and the siz of the Department of Defense who is going to come back and write this plan and even present it back to OMB a little beyond the 27th. So may be there is questions at that level and also as we start taking the requirements apart who is going to do it and who in fact is actually responsible for some of these things. Because for those of you, once you put a smart card or a minicomputer in the hands of every single member of your department it ends up cutting across very, you know huge bounds and it is trying like an axe to the infrastructure that exists out there. So we started putting this together and trying to decide how we are going to answer and also who is going to be responsible in the department next. There are 212 paragraphs in the FIPS 201, what we did is we disassembled those 212 paragraphs and we came up with 30 pages of requirements. Those 30 pages of requirements are broken down into those numbers right there. 135 of them are satisfied by our program today or just require some minor tweaks, easily do 69 of the requirements rapids is our ID card issuing station. We already have a redesigned underway, which has been underway for a year-and-a-half, which we will start rolling up probably towards the end of this year, which gets rapids up on the web and makes it much of a web client and in there are either, in there already or we can integrate those into that software re-design. I think as all of you know again in the Department of Defense for those of you because this does cut across large areas of the agencies, either the Department of Defense were not solely ___, my organization is not solely responsible for implementing the FIPS and as you know, even though you may be in the same department and whenever you got a partner, you hope is a strong one, okay, so that is the _____ things. We got to like work with our partners and figure out who is going to do what cases and when they are going to sign up and how we are going to match up the schedule. And three requirements at the bottom, one of these an example of this is it says that you have to be absolutely sure that there is no way that anybody can issue a fraudulent credential, that is the requirement in the FIPS. So our choice was, I mean that’s a hard one to do. So one of the things because we fought very hard, because we only wanted to have two physical human beings in the process, so our choice was hire another person to watch the other two. We felt that would be the requirement, but what we have chosen to do in that case is we are going to put a lot more audit requirements on the workstation and on the credential issuing process and automate those in a lot of ways to the credit card companies do again. So a lot of what is in the _____ is a commercial implementation. It is very much like banks would do and you know we try really hard to go back out to the commercial guys because many of them have done this. I will say that as far as an identity card, we are probably one of the larger scale ones that are out there, but there is still much to learn even after five years. So from those requirements, we had 17 items, that we really had no idea how to go forward. So our organization over the last week, we generated 17 white papers, this started out applet changes, and reporting to report, report back to OMB. The resourcing impact I think our physician is, there are things that are in the FIPS definitely going to cost money, however, many of those we supported through the entire process because the Department of Defense felt they you can do this anyhow. They strengthened in the security partially out, out there and we have seen rare people who are are expertise credentials and we feel this is something that we need to do in order to protect our troops, both in the United States and overseas. And the last one is one that do describe and Judy will help me with is to who is the letter going to in your department and from there who has actually going to be in charge. I think, _____. Lots of people think there is going to be a lot of money attached to this, so when that happens, there is a lots of people who suddenly want to be in charge. I think my office is going to end up doing a lot of staff work. I just wish one of those guys who wants all the money who wants to do the staff work too. So have you found that guy yet? So there is a great deal of work to be done and for some place the size of the Department of Defense as an example. Right now, we are not necessarily taking electronic fingerprints on people as they come in either as military or as civilians and definitely not for contractors at point of entry to give them credential. So that means we are going to have find a way to electronically capture the fingerprints and get them vetted through the FBI, it seems sort of answering back, it is going to be good enough for us to provide a credential. Right now our mark is we have just did up a central issuance facility that we are going to use it for the recruit training centers. So we have promised the recruit training centers that we will get them a card for those members from the central issuance machine within 72 hours. So that’s our turnaround point.

So, what that means is every single military entrace command place has to have a machine that is going to take electronic fingerprints, the process to move those to the FBI and how that is going to happen has got to be sorted out, who is going to pay for that and who is going to be responsible, and right now, we still have not figured out who the guy is we are supposed to be talking to. So, those types of things when you actually get down, really I think, we really look at this as being two to three years worth of work for us and I guess I just said that. However, I do invite all of you as a member of the IAB since it started I guess I do not know how many years ago. All of us now have a common set of requirements for federal credential. This is a chance for us to act as a federal enterprise together. There has been lots of work done here and I will tell you, this is not a pleasant job to do, okay. For those of you who are going get the job, it is not a good job, okay. I really learned that from the head of the New York Board authority like issues something like 25 million cards a year. Cards are not a good business to be in, okay. Both our department and through the IAB we have done a tremendous amount of work and there is going to be things like training, there is going to be things like technical documentation, there is going to be these types of things where my belief is we should not all go out and hire our own contractor to do the same thing over and over and over again. If we have common requirements my office, my department openly says through the IAB and will share whatever we have with you. And, I would just tell you, we have made every single mistake you could make in this situation. It has been painful and we could help you if you choose to listen.

As part of the next IAB meeting, I think the date is being kicked around right now, my office right now is buying cards for other agencies that are out there including, I think we are starting to, we are working out the details of being able to buy cards for some of the states and the DC government, 13 states May 13th. I thought you had lot more states, maybe 13. So, but my office right now owns the contract. I have a lady who will help you through that and our office is also trying to put together the requirements for this aggregate buy so that all of us would be able to do this as we need a new contract by summertime, I believe, right Darwin? Is it still the summertime? Like next month, right? So, okay.

The next one is something that I have a plea for all for you. In our department we have a physical security system that we use. We have over half a million people registered them. It uses a hand held that uses a wireless access back to a laptop computer. It is used extensively overseas, the Korean peninsula is being stood up in Europe, it is being placed in both Iraq and Saudi Arabia and it is also just started to happen here in the United States. So just within the DOD I have that that hand held for my program. We have another hand held being introduced in Iraq that is going to take fingerprints on Iraqi nationals who have access to bases. There is probably a couple of more examples in the department of defense. The first responders community has a hand held that has some unique capabilities using PKI. So, I have been offered from, I am not sure how much yet, but from our homeland defense undersecretary some support and what I really want to do is, I think that putting a plea out to really to capture people who are especially in the law enforcement community so that we can build or at least lay out specifications for industry to build us a hand held that could be used for police officers but also the meet the needs that I have for my military police in overseas. So, I do not think that exists out there today to the requirements we have, but this is what the FIPS has brought to us. Now we know exactly what numbers are supposed to be transferred back. We know that there are certain technologies that will be used to transfer those numbers, there is going a contact card, there is going to be a contact less card and that is going 14443 contact list. Those types of things allow us now to start building the tools that we can put out there to help protect and increase the physical security of our bases both in DOD but also for our federal government and in the Washington area and for the cities of United States. That is what this about. We have some issues with the FIPS that we would like to work out with our partners on logical access. One of the things that was not strongly laid out in the FIPS was the back end validation transactions. So we would like to be able to talk to technical people and this is something that is going to happen over time to lay out what the technical requirements are to validate the card and validate the credential. DOD already has a web service that does this, but it is also going to have to be modified and I think all of us need to sit down and do these types of things together to get the data flow right. Otherwise, we are going to be sitting at meetings like this for the next 15 years. We have some questions about how the data is going to be put on the card, now that we do have the FIPS and some questions where I think we all need to agree as a federal enterprise of how this is going to work for our people who are out there using these cards and credentials on a day-to-day basis. One of the things the FIPS says is the serial number which all of the cards that have been out there today, the serial number if you look on the back is in upper right hand corner. Now theyhave moved it FIPS to the lower left hand corner. That is a big issue for our card manufacturers because they told up in order to do that. Someone asked the question, is this something that we need to do to help our industry partners who have already been supporting us and this is one of those things that slipped through, we need to make some decisions here. Our folks on the west coast would like to put together a low level developers guide and I would say that industry we now count the federal government and are the first responders, states, local government into this. There is obviously a market here to build products that we will all be able to use in future. So we would like to get together. I think, my agency is willing to do a lot of that type of work, but we would like to have some help from other folks who would qualify that are out there because this needs to be a team effort and it really does. And the last thing is we have started this with the IAB. We tried to put a set of documents together in the document repository for people Judy has provided some contract support that will help the IAB. I would like to get this stuff up on the web and for all us to agree that this is really where we are right now. Not only for those of you who would not want to use them, but you know, right now, I have been asked to sit down and start talking to states to transfer at least the knowledge we have to them and there is only so many of us and I would just tell you this is extremely technical information and there are not a lot of people in this country that really understand this very well even if you go, you are going to have trouble hiring them. There is not a lot of them. So, we would like to put lot of these together. I will tell you, I have the best staff on the planet earth and I will also tell you, I cannot say this enough, from my department and also because we worked together as the IAB we will do whatever we can to help you through this. You just have to ask.

That would be me. One last thing, they took my regular e- mail off of here, it is michael.butler@osd.pentagon.mail. What this does is it goes into our mailbox and the staff sorts it out to people. I just had my entire office contract staff changed out last month. So either use this, or use michael.butler and just be patient, it might take 48 hours but we are all there for you. Thank you.

One thing you noticed that Mike did was from the HSPD implementation to states and local in the first responder. Why HSPD is out there and we are in support of that. The IU\AB is actually a broader partnership. We do have the state of Pennsylvania as a voting member. We actually have the the National American Public Transit Associates as part of this implementation, so why that the federal credit or _____ is a part of this platform and part of this _____ that we are talking about this week. We want to make that work in conjunction with this entire architecture that were helping rule out way beyond, if you will, HSPD 12, so thanks Mike for bringing that up because we need to realize we have a broader audience to serve as we are going forward to as well as this audience we are trying to address today.

Tim: At this point, William bring charts to talk about _____ program in general, but what I like to do is to talk a little bit about the role that I have had in the technical work group and coordinating activities have been done in developing the IB responses for FIPS 201 review and 173 review. There is a few points that I think I might bring out in terms of merging what I have not had experienced the program we have been working on at NASA and the general high level things that I think are good to recognize and trying to divide up your level of effort in where you might be able to assign responsibilities in meeting all of the different requirements that arein FIPS 201 because it is not just a technical instrumentation, it is not just a policy implementation. You are really talking about significant culture change. My assessment of having looked at our organization and having others described their organizations in the way that they have conducted business up to now. We are really moving out of paper base process when you go to PID 2 to and so my perspective in the role that I play in our program is looking at the technical implementation, looking at the commitments that we are making now in terms of our infrastructure investments, so that when we get to PID 2 that we do not have to go and replace something that we were able to do today, as I had mentioned earlier this morning, there are some things that we are able to do today that we were not able to do as shortest two months ago, so having said that I will reiterated that having identity management system away that you are going to be able to track enrollments, applications and realize that civil service are going to be treated differently than contractor enrollments. We talked about involving HR or HR works real good if they are civil service employee enrolling in a civil service identity badging system, but if you got contractor staff coming in, typically you do not have an HR involvement with the contractor that you bring in. You are going to have contract relationships there is specifications that are hard of their contract issuance of information that are going to be provided for the contractor employees that are coming on, but from the standpoint of the record keeping, the information that you got to maintain in moving forward, you going to have to have similar information, so the basic guidance you see written now is that _____ as of 85 or as of 85Ps, this is the typical information that you would need to collect regardless of its a civil service employee or a contractor so you got contract in HR, you got IT involved because IT is usually providing the services and there is some integration effort and level of service provisioning that needs to be involved in IT. One of the major COTS items that I see that comes up here is that you got to have a electronic workflow that allows you to keep track of named users as were in the licensing jargon able to track the applicant, to track the approvers, how you manage your approver list, within your electronic workflow, because if you are not doing this electronically, I do not know how you are going to keep up with the literally millions of applications and fingerprint requests, photographs, things that have to be done in an investigative process and where he now working in the security area primarily, so you move from the first box, which is HR contracting and possibly security into the second block where it is largely doing the NACI and so forth. Then, at that point you collect all this information you have ajudication has to take place so that the individual is trustworthy to issue the credential, then you have the actual insurance process and in the PIV2 implementation, you got to carry his finger prints or the picture biometric through this process and make sure that the person actually delivered the card to in fact the persons matches the biometric to the persons that was investigated. This is the piece that has been overlooked a little bit. I think in the planning process I think it is extremely important that you are very cognizant of this requirement. You can look in FIPS 201 and section 5 and subsection 2 and 3 where he talks precisely to these details. It is at that point that you actually have credential in hand. I will say that having the credential in hand is only the tip of the iceberg. He had the identity management problem in the beginning. He had to do the investigation and I got a credential. How are they going to make use of this?. So, I have talked about three significant areas of effort in terms of design, deployment operations. Now, we are talking about how you are going to turn around the and use this card for logical access, and physical access are too very, very large areas that have their known near challenges that have to be addressed and typically addressed in very different ways. Historically, physical access does not have a lot of IT development. I think it is very common for security to have gone and obtained their own IT support services that are sort of integrated in with the security types of contracts that are put in place, so it does not always have the same IT oversight that you would have logical access or your web presence or any of financial systems and bringing IT into security into the sort of closed environment is a challenging effort at times, but I think security is realizing that this is now a kind of moved into really IT Centric kind of technology and that they are not well equipped to deal with the sorts of things that are going to come up and smart card based physical access control system, so I think that once they understand what the requirements are they are going to be very receptive for management and IT oversight coming and they help them in those areas. Though, logical access and I think DOD has set the platinum standard here. I have been able to go in with cards and the large deployment and do smart card log into the workstations. I have not been seen anybody that has done a quite in the same scale except some private companies have done it, but have not crossed organizations like we are talking about now. Standards are the critical component of making this happen and what I will say is that there has been lot of very talented people from industry and from the agencies that have been involved in writing the comments that NIST has incorporated in English standards and I think this is a good product, but there is plenty of work to do to get us to the point where we can actually declare that is all working, so having said that what I am trying to do is get you to think a little bit about questions you might be interested in asking.

Kevin, what’s the world look like on your side of the planet. You guys are ready to run I understand, allegedly so, point out a few things about our, I do just experienced today, as I talked about earlier, we did have a couple of smart card implementations in DHS we're beginning to leverage, but one of the largest things that we did was we created a program office to try and corral all the various components and functional areas that you are going to need to pull together. We talked a little bit about IT and in our case the chief information officer collaborating about that. The people need to bring in to the _____ goes far beyond that and a need a single office that will manage that, so we establish the joint office identification _____ for DHS that has the responsibility to implement HPSD throughout the _____, obviously very large undertaking and at this point, we have little staff _____.

But our intent was first to provide the structure for the organization and talk about responsibilities that, that the organization would have from marketing to communications to the actual technical support that the CIO provide to us and then, but the requirements have generated from the program office, which is the way that we felt would be easier to structure that and it made a lot of sense. Recently we stood the office of the office security as for the, the headquarters component or model such where the office security manages most of the hazards that are brought into the game as far as this process is concerned. If you go back to your own organizations and you look at on what you're doing today, you are doing a lot other things that the requirements called for today. You’re issuing badges, you’re vetting people, all these things happened today. You're, you're challenge is to see how your current process is now migrate into what's, what's coming up with the smart card. The area of the expertise that you are going to search for those, the card management and all the things that are smart card related that may be new to an organization. When ______ first came about, they were _____ going on at the same time. We collapsed those into just a couple and then from those two, we are going to try and pull together, you know, the best of both. The headquarters implementation focused a lot in the cyber side, the ability to, for a person to come in for enrollment and receive both their cyber and physical access, when they are enrolled to and walk out of the enrollment station is going to use their card right then. So, that was, that was key for us and so we did bring physical into the game, but within DHS, the _____ card really looks the physical side great things on as far as that technology is concerned. You heard, earlier we talked about the enrollment stations and how we have to capture fingerprints and have a clear chain of trust in all those things involved, but we have technical solutions and support that now. Our challenge is to bring those two solutions together. You'll have to have a technical solution for this chain of trust and set up before but that, to me that’s, that’s really the key to success for a lot of what we are going to do providing the chain of trust, being able to track the individual from the time you offer the job and begin to fill out their, their 85 or 86 and go through the vetting process until they show up and receive their, their credentials and then start work. In the headquarters, we, that process has shifted for us, we have, we have all the pieces in place currently that will support that. One thing that the FIPS tells us to do is now we are going to have to capture photograph biometrics up front. We are going to have that as a separate process now that where we capture the fingerprints, we do capture them electronically submit to OPM but then we don’t take he photograph for any of those in the personalization until the person shows up, so there is that short disconnect, you know, _____ that we, we have made it so that process is connected to where _____ talked about the person who actually administers the card, thus a baseline information _____. That information they have used are created, you know, _____, some process where you can chose your badging office with over the phone and with signed by someone in the picture and receive the badge and that's the process that we are obviously trying to get away from, need to have that, that connected, connected that chain of trust, that not only our card we will, we will provide, but also the cards from everyone in government. I would leverage. You are providing badges to pretty much everybody in the organizations. The PIV is only obviously for _____ contractors, but you will have situations where you have to provide other types of badging, so your current badging that you do now there is still be a need for the people that will be outside the communities that will require this, so you need to kind of keep that in mind. You really want to go back and look at the structure of this, but look at the structure of how you are going to manage things that are going, you’ve got to pull everybody that is involved in. You need to try and do that centrally so that you can have a collective message, collective of strategy, you’ve involved everybody and engaged, everyone is going to be, you know, part of the process, which is pretty much everybody in your organization, you know, from finance to security to IT all of all these folks have to be involved and then from that, you get, you know, you come out with your best solution. As Mike said DOD with us, so we need not have to really start from scratch, although we were, you know, the new folks Joe worked on the _____card. We learned a lot of things from that. We had a lot of lessons learned from DOD and _____ for us that, that we leveraged we are going to try to go back in and _____ might do with your, with your new organization, so we try to leverage what other folks have done and plus put, you know, put in the latest technologies that we know at the time to try and pull our project together.

We know about the time to try and pull our project together. One other thing is as you heard you will have to submit a single plan from your departments so, I do not know how you all of you are structured but we have several components within DHS that we have to pull in to make this plan solid. So you are almostt going to have individual plans from your components organizations. They will have to come together and combine with the overarching plan that you have to present to OMB. So the data collection is going to take sometime and you are going to have ask the right questions to the right people and that is going to be difficult to do. For us we tried to go to back to our original Innovative Project Team and start with them and then from there we are going to expand it to make sure we you know, got the right people. As you can see now there are still memorandum and things to come out down a CIO path since Smart card has been a traditional CIO project that, you know also security might not be aware off, or _____ might not be aware off. So you really need to get that co-mingling of functional and business units together so that you make sure you get everybody involved. Some of the policy challenges I think have come out in dialogue and I would like to try to provide a little focus so that we could actually talk about some policy issues that we are going to need to going forward. I know that applications just like buildings are usually security centric. Every application that we got a hundred and they all have user names and passwords. Is everybody familiar with that, is anybody not familiar with that. Does anybody have besides DOD an enterprise, we are going to the applications level, you guys do not get it do you, yet work, but not an application. So we actually organizing some additional policies as we go forward to fully, if you will take the power in the logical side, and take it across all our application to make everything if you will through one process ____ compliant, it needs all the FIPS security certification and the creditation. And huge cost goes into every time we bring an application up, we bring it up in a stove pipe sense the way we currently bring it up, there is huge cost associated with that in huge risk because most of those user name and password based systems are level II and are really, you know security is an interesting word to use at level II. So we have some policy changes in that area, likewise I know Mike, you and I dealt in physical space, f historically physical security was building center and I again from policy issues, in fact it is mind boggling. Now that we got the _____ compliant, I do not know how we would open the doors of any new federal building tomorrow that does not atleast stipulate FIPS compliant readers at the doors. I mean that is a policy issue that is working its way through at the federal level, but can happen. We actually have it in our inside out bureau and our department that all new facilities will have to have readers to be able to read these credentials that we were issuing, and we have a forward migration strategy.

Mike, I know that you guys have been wrestling whith this. use what have done and in your policy area to make sure that you can go forward across enterprise, actually use this tool.

Well, before I go into that, Want to take one moment, Charles. I got both the incoming and outgoing _____ of the IB and they both been stressing the need for involvement of all the agencies and what I would like to bring out is one fact that the IB has been very instrumental in certain aspects of putting the FIPS together. One of the key reference documents in the FIPS is the pax-202 and that was basically put together under my working group which is the physically access and aids by interoperable working group, but one of the key architects of that document is sitting right over there, Mr. Tim Baldridge and that with a whole group of others both in Government and industry worked for a long long time to put this document into some sort of order and pass it up through the IB and up through to FIPS to get approved and it is now as I said one of the baseline documents in the FIPS and that is why "involving the IB I think is very important". Now to go and answer Bob's question on policy. In the state department, we have in the past been sort of introverted. We were only concerned ourselves like most agencies and even within the State department, we had really two realms that we have looked at. We have had domestic operations, we have overseas operations and up until very recently or under extreme circumstances, they never came close to be in associated with one another. Our present Smart card program that we are implementing was primarily dealing with domestic issues.

We were going to take care of all of our domestic facilities both within the national capital region and within around the country like the UN in New York, that is a State Department responsibility. We have got a major financial Center down in Charlestown. We would like field officers all around the country and that is our basic concern was. The overseas mission that was left to overseas group, you know as I said that we basically never came together. Now things are changing and this change means that we have to now look our policies, and our policies are going to have to be modified to incorporate these changes. An example, of the 207 missions overseas, but that at least a year ago there was about 18 automated access control systems deployed and of those 18, there was about 12 unique; so that in itself was a challenge or is it a challenge, every post was using their own type of badge, they put their own _____ now of our smart card and some use magstrips it mostly over flash passes again totally different than what we are doing domestically. About two years ago, we started to the issue the smart card for domestic. We started a dialogue with our overseas people primarily through the fact that we had a PKI standing up and we have to get that PKI around the world. To get it around the world, we had to start issuing this smart cards because that is our platform, to do that we work with the PKI office. They began issuing smart cards at all missions overseas and we have not even completed that yet. We were still in that process, now with the smart card overseas we have did just want a issue of a blank ugly looking cards, so the overseas officers created a what we call a glide card or global look ID. It will basically resemble what exactly what I wearing around my neck right now, but it wont necessary have all the physical access capabilities assigned to it, but it will have PKIs certificates, so therefore as PKI rules out that at least all of our employees both domestically overseas we will have this PKI. Now, along comes a HSPT 12 that is starting with change things, what ever we are going to do about it we got to do domestic and overseas but to how to get every one together. What we decide we have to create a sort of board of the directors we want to use that terminology and that is going to be of the key stake holder, bureaus and offices that is going to include the bureau of diplomatic security, which on under bureau of information resource manager or PKI or CEO. HR is going to be under HR if they need money or we are going go through. We have five geographical bureaus that all the embassies and mission of overseas fall under. We are going to have to have at least past of that involvement. We are looking at other officers at what roles they might play to get involve in this board and now board is going to be a high level board. We would look at a deputy assisted secretary level or may be higher. We wanted to be oversights board. We want that board then to create working groups and we will create three basic working grades; one technical, one policy and one personnel to start ironing out all these issues and working on time lines to put these issues into places both domestically and overseas. We have got a big road ahead of us. We have got a major cultural issue to overcome. Again, overseas culture is totally different than domestic. It is 99% well maybe not so much as that 95% all foreign service. Domestically, it is primarily civil service with a large or small foreign service contingent. We have different outlooks for missions impart between domestic and overseas. Overseas security is different, I said earlier today, we are concerned about contact list and biometrics cards because whether be friend or foe, targets. We have always been targets and this is even worse now. We have number of tenantts that serve that embassys, practically every embassy we have. We have the IRS, customs, which now the adjust would be _____ officers that some of our missions over since we have a multitude of different agencies be presented at our missions overseas. This is going to create issues with the FIPS being deployed within the different agents, how we are going to implement interoperability. We having other issue that lot of agencies that look at. We have a network system some intranet its is close that has one portal to the world, so if you are in Timbucktoo visitor there, that is not going to go on the internet, that could have to come all the way back to headquarters and we have to find a way of communicate from headquarters to whatever we have got authenticate that individual, so this communications problem, networking problems is that we have to address that I don't think as really been brought up yet. If within our organization that would not be so much but we are doing cross organizational authentication that is little major concern and it has to be addressed or we are going to stand up at the PKI bridge. A centralized CRL list or some thing of that nature were if Mike comes to state and puts a finger on it. It goes automatically after that location. Is it going to be a Dollop, is it going to be direct access. Is it going to be an internet connection. There is a issues that we have not even approached yet and that is just for here, to apply that overseas if we have got this close to that work and then speaking a networks state department or access control or the domestic side has been closed off for more regular intranet. So we have our access control system has been locked down and closed we don't want to know on to get into it what I have to change now that going to be a policy issue, how can I issue a credential that is going to be a PKI sign or certificates put on there if I don't have some sort of connectivity using my intranet or PKI resides, so we have got an issue of now having to move some of our physical access systems over through or intranet or PKI resides, so we have a lot of work that ahead of us, but these are things you have to look at when you either developing from a start or if you already got a system you are going to built into it, but we have to look forward too. We have to get management buy in up to this board. If we don't get management buy in is just an another in the state department they look at as a DS project and no one wants to touch it. This is not a DS project, this is a state department project and every one that involved has to get involved money, this is not will come out just our budget. It is going to come out of this state department's budget now. We are going to come from _____ office try to get involve. We are talking about involvement of an employes. We have the issue not only of government employes and contractors and goes along with what Kevin said or with Tim. RHR primarily right now take care of just the government employes. All the contractors are vetted their own company and lessen over to an another own office within the _____ security and then process in that way basically a bypasses HR. HRs are now staring a program, where we are going to try a capture every one into a database for emergency notification and we are hoping to get all government employees, all contractors and all foreign nationals around the world, so if this really goes through it as they expect we are hoping for then at least to have good database of pertinent information on all employes. I meant that could be fed into our physical access control system and issues of tokens and cards be assured in the proper mannerism, so we are looking at a long role yet we have do not have much time. We have been issuing cards that I said for approximate two years now, that means that the card we have will not meet the PID in its final stage, because it is a single chip contact card and PID said that we are going to have both ____ so we know right from the start. We are going to have to replace every one of our cards, well that is a cost but since we are already have funding for the cards.

We are hoping that we can get the new cards and start issuing them before that October 06 deadline rolls around where we just flow this into a normal procurement cycle, but that something we have to workup, the infrastructure we had I have mentioned this earlier, we have an old Reagan card system for lot of our systems. We were replacing that. We have got just about 80% of our headquarters building, the areas Truman building and about 13 to 4400 annexes converted over to the new access control system which will take the smart card readers and we will change the system altogether. Well that takes money so, we have to fight for budget. This year like every agency we all got hit with the pretty bitg cut.

_____ along those lines and we are going to get the questions here in the audience quickly, but all of us on stage have been implementing smart cards with only internal agency policies. I know that _____ letter was signed 1999, 1998, we signed our letter I think two or three years ago where we actually published the policy. That said they were implementing smart cards throughout department of interior and that similar to the struggles that we all were facing as we were going forward, but now we actually have this external requirement HSPD 12 which will help us as we if you well FIPS to get funding, is no longer hopefully going to be the same struggles we have faced in the past with us doing this a long as an internal business process. We have if you _____ external policy, they says that we all have to do this. So going forward we hope that these new policies that are coming out should help us along and it is being dealth much differently than what is being done historically. So I think hopefully that will help us give forward. You talked about the policies that relate to physicals, logical. There is a MO-404, How many of you are aware of the MO-404 document out of OMB. You are going to look at that, that is the policy statement _____ sometimes this next October and November time frame that we are supposed to do certification or supposed to do risk assessment again our entire all of our application and decide whether or not level 2, 3 and 4. Level 4 credentials if you will, this is the level 4 credential and level 2 is the password so we actually have some policies that we have to answer to that, we didn’t have before in the past. With that I think it is question and answer time for the audience. There is two questions that came in large stacks, one have to do with the NACI. There was more questions on the NACI than anything else. We are going to get to that, but I would suggest that the NACI and there was another question relies the trust, however we are going to trust other peoples credentials. How many of you are in the GSI building today right now. How many are you here?. So, evidently there is some sort of trust that already exists if you will, what we are trying to do is not only raised that trust, but bind it, if you will through these other process so where we can actually trust more. I think we already have a certain level of trust and we want to raise that, so those who are the two biggest pieces that we have gone so far and questions. We are going to get specific answers to it.

Okay, one question I guess this for DOD and may be some other agencies foreign national visitors got to do it. We have in our agency commerce, let's say, plus and minus of 1000 foreign national visitors that are here with us for about anywhere from six months to two years. They are not cleared, so we are not talking about NATO clearances or any other that thing. So, the standard says that they have to have an investigation, a NACI, there is no such thing as a check for public for instance okay, but we are going to him a credential that allegedly gives him logical access. We are going to allow them to have physical access, unencumbered with escort, we are going to take our US folk and send them through a lot of pain but we are allowing the foreign visitors to go without an investigation, so I am just curious how they all may be dealing with that as we tried to implement the standard. I am trying to answer that and that is one of the things that I helped bring up the thought I brought up this morning was not all the answers, but the questions.

One of the things I thought I brought up this morning was not all the answers. I am sure that the panel will give you their best of their answers there, but we are going to as the IAB put together a group that we hope you participate with, so that we can better get a much better handle on a cross government not only from the Department of States Issue or the department of energy has that same issue along with several others that we could help solve this, which is a very, very complex-type issue, especially when you are dealing with somebody from the Czech Republic, not that they are bad. So I don’t know if anyone has the answer.

Do you have the answer Mike?

No.

I know I have asked Mike Butler of the DOD a young lady sent an e-mail saying that he is willing to share what their polices are right now, not that they should be the future polices, but at least that should get us any other agencies that has those type of polices on what they do right now. We will try to merge that all together and forge away ahead and recommend what is the best way forward. We will take that on as part of the IAB. You know, I am sure that somebody is going to take this issue on and the more we participate, the more we will probably carve out what the future looks like rather than just have someone bestow that on us, that makes any sense. Now, is this is the time want to add anything today?

Ya, I would like to add one thing. This issue that you have got is bringing foreign nationals into the country and we talked briefly about this, and I have talked this with my superiors in the department. The State Department would not really get involved on that, because that issue does not concern the State Department itself on this side. However, our Consular Affairs office, they issue the visas oversees and depending on what type of visas these people are brought into the country on, could you determine what type of check is performed on those individuals, and what you might want to look at is what type of visas these people are brought into and maybe we will have to change that visas type. I just _____ would not want to do this, but an immigrant visa is going to require a greater background investigation than a standard visitor visa, which is probably just a rubber stamp. So that point about foreign nationals coming into the country, I have no honest answer to give you and I checked with our people may have no honest answer, however, when you talked about someone like from the Czech Republic, we have an issue of those employees in the Czech Republic. How do we do a NACI on those people? They are working for us. They are going for DOD. We have policy written that says what basically will do, but it varies from country to country. There are a lot of countries that when we go into, we hire through the Foreign Ministries Office. They give us the list of employees that we are going to hire. I don't care what we do that person is squeaky clean as far as we are concerned. So, this is an issue, this is an issue, and I do not know how to address it on foreign nationals.

If I can add just before we go to the next question for those that have not read it yet. The current DHS authorization bill has some very interesting requirements about how we are going to vet things and what we are going to use for investigation process whether it is for a traveler program or a voter management program or just general programs, but there are supposed to be a consistent singular vetting process. Mike you are on the money for folks that are already in country depending on what type of visa they have very much will determine how much background work has already been done on them, and getting a handle on that is not an insignificant task right now. (audience -inadible)

I do want to say, I mean, as we were doing the _____ and I think this is right. I have read some new versions of it over the last few months, but I don't think it included anything outside the United States at that time. Okay.

I do not think the FIPS itself has a requirement for outside the United States, however, that is it. Okay. If you are going to do this and you are going to use your physical security systems over there and we all have to deal with these people. I mean, we have to find ways to integrate this into our existent policy. It just going to be one another thing, this is an interesting group of folks we got to figure out. The other one that we have wrestled with for four years, which all of you will wrestle with is volunteers. There is another one it is like a tough nut to crack. Mark ____, HHS: We recognized that the background checks are going to be a little bit difficult, somewhat time consuming and cause money. My question is since DOD pointed out the your staff is probably some of the best and brightest doing this, and lets assume for the sake for argument they are full time employees. So my agency managers they have gone through the whole process, manages to talk them away from you and come back to us as a contractor. They leave you on a Friday, turn in your credentials everything is revoked. They show up at our badging office on a Monday. How do we take advantage of the fact they have already gone through the vetting process, which the sharing between agencies, so we do not have to do it again. (audience- inaudible).

Our understanding is that OPM and we will make that is available.

NACI change condition OPM maintains the security and suitability investigations index right now. Anytime, anybody requires any sort of investigation from us, that fact is recorded in the database, and a check of the database is also conducted on any subsequent investigation that comes in. So, if that contractor is coming from another agency that requested investigation or in fact did their own because agencies that do their own are required under the executive audit report to us the fact that they are in fact conducting one for inclusion in our database. So, we have done it or if another agency has done it that should pop up in the database. Now a lot of people in this room are not from personal security shops I think. _____ personal security shops and some of the _____ shops can access OPM database either through a telephone call or direct system access at their office bases, and determine at the click of a switch whether or not a certain person has had an investigation and if the information was reported accurately and timely what the ajudication result of that case was, so that's the system that exists now.

We are under certain mandates from the NID to add information to that, but today we should be able to do that. Again, assuming the information has been reported properly into it.

My name is Julie Hunter. I am with the Center for Disease Control in Atlanta and I just wanted to make a comment about the foreign nationals.   you will have problems we have them to come in our offices and use our labs for years at a time. you can probably identify with that. And it depends on the type of visa that they are coming in on, but we also have to FBI liasons that work out of our office. And we also have 2 former FBI people that work in our office under our jurisdiction now. So we have the links back and forth with FBI. We always run our foreign national names through FBI as well as checking of course the visas that they have and in what entity they are coming through whether WHO or whoever.

As well as checking of course the visas that they have and what entity they are coming through, whether it _____ whomever. When they come in, they work, you know after the clearances are checked they work sometimes in _____. So it can work and then also I decided about OPM. We worked very closely with them out of the Atlanta office. They are very helpful. We can get almost instantaneous answers on clearances as he was saying for contractors or FTEs that are coming from other agencies and it works beautifully where we are. I do know you know what region you will be in, but it does happen and we use that everyday with our personnel security area.

Janice _____ with the Bureau of Indian Affairs under the Department of Interior. Now with the National Agency Check, OPMs requirement is only to send out the vouchers. I am receiving NACI reports where they are no responses, so for me I am not comfortable in accepting the adjudication of another federal agency if they did not have any information. There is a special public law that the Bureau of Indian Affairs and the Department of Health and Human Services, it is the Indian Child protection and Family Violence Prevention Act and that requires, in addition to the Federal and State investigations, also local law enforcement checks and that is not a product that is available under the NACI so for me that is still going to be a concern.

We are going to take a break. No we are not going to break.

For those of you, who have an existing smart card implementation, what is your strategy for migrating to FIPS 201 compliant card and system.

First of all the common access card does have to look at the physical changes, one of the decisions that we made when we started five years ago was that Red should be foreign national so that’s why we were using that for and the FIPS now says that Red is first responder. So we could not have been any more 180 out than that, so one of the things that we are going to do and we are also including probably adding some security features to the card, which is something we wanted to do for a long time, but because our card for military members is also Geneva Conventions Card and access their passport in many places in the world. Whenever we make any kind of minor change in the card, there is a huge PR campaing that has go through the State Department and most of the countries that we put our people into. So that is one topology. If it changed we would probably do that some time next year and that is really the major thing that we have to do with the Common Access Card. On the card itself, and one of the white papers that we have talked about is how do we actually implement without having to impact one of the big impacts that you have to consider is the middleware that in our case is already been funded. We have 2.2 million computers in the Department of Defense. We never knew that number till we had to buy the smart card readers and middleware form. So that is how many are out there. We have done a lot of work with middleware standards and requirements and the Department of Defense has a contract. It has been in place for a couple of years. By the way before you buy middleware, find out how much we pay for it because that should be your marker now just leave it that and that is really our big impact. What we have got to try and do is to put the requirements of FIPS on the card and that may require, that is one of things what I wanted to talk to the IB about is do we want to do this aplet and how do we want to break the data up in order for it to work properly. So that is the decision we needed to talk about. The ones you get off the card is the back-in systems and how we are all going to transfer data back and forth through each other. We have a lot of these programs in place which we have put in place and based on our thought processes, but through the first responders you know we have come across people like NIMS who is trying to come up with the database for first responders across the country. You know, we have a lot of first responders. So we are going to have to sort some of these things out and all come to agreement here in the future and many of these people who has just stumbled on in the last few months so and also Driver's License folks and things like that. Mike or Kevin. You want to respond to that question. For us it was more of a situation of just evaluating what we already had. Once the standards are in place, once this was released _____ then we were able to take dose specifications look at our current metalware and our implementation and they make those changes so our _____ site they have been in, in the lab making those changes to our implementation currently we have a version out now that were in the process of testing. So we did not have a ton of volumes. We did not have that issue plus the readers on the access control site above this _____ we did not really have the legacy issues to deal with. So they were already fairly compliant. Our biggest issue is more than data model and those type things that we needed to make sure if we were able to capture the correct data that we are going to need to put into the new data model that the 73 requires. So not a big leap for us. We have already designed the middle ware ourselves.

Michael, I agree with what Kevin says, the one of the issues we are going to have is the card that we issued. I agree with Kevin right now the issue that we are going to have in converting over to FIPS 201is the cards we are issuing right now. We are installing and coding the card with the _____ of the DOD. The _____ say that we are going to use _____ and that _____. We are going to have 1000s of cards out there that is not going to have the _____. We are going to have to come up with an approach of either changing out that card so it will at least work as we upgrade our system or we are just going to have to float those old cards out in the field as we incorporate the new system but I see that it is going to be a little bit of an issue. And for us on the physical side, we are going to transition from magstripe readers that we had _____ right now will be of the _____ on the new card as we transition from that reader to the new compliant readers. So I would say the most significant _____ base is the OD in the four million plus cards. What the issue today is they have an install basis of 32K. They are moving to _____ card anterior _____ is a contact or contact less card that they have out there in the 1000s, not the millions if you see that. There is _____.

We have processed only 60,000 cards issued worldwide right now. So they are some agencies that have, each agency will be dealing with their installed base differently but my suggestion to the answer to your question is that if all the agencies through the IAB working in common as they hardly migrate from where they are to where they need to be that there will be a significance in what you invest to do that by and in also what it would cost you to acquire to install that base. So I think through the aggregate buy and the wisdom through the other agencies you can go from where you are to where you want to be rapidly and with significant cost reduction. I do not think that there is any buy in this town that can tell you that the front ends of the process meaning the identity vetting all those pieces that we want to do. I think there are some that are gone through, like for example Donaldson has gone through putting a process in place on how to streamline that. There are technologies that need to marry current management system is in spec. I would say that anybody who stays in this town that an AGC has that in place, they are lying, but collectively working together I think you can get that in place rapidly if you work together towards that end. I will get off the band-box.

My name is Tony ___. My question is regarding a logical access requiring PKI definition of global workstation and remote network is what is the definition that we were using for local workstation requiring to it _____ versus the definition of the remote access that requires strictly PKI. What is the difference between those two and where is the line drawn with the systems requiring PKI. I know it is based on the assessment done for authientication and what level of assurance this system requires but is kind of confusion.   and what level of assurance the system requires but it is a kind of confusion. At the best PKI guy but I will just stay from a high-level view point, I think our position is that we want to have cryptological log on for folks which working towards in the offices right now, people are working in the office. We do have some people who do have a common access cards they use for remote access and when they are in traveling things like that. I would not say that that is a common thing it is out there today, for instance when I come on to OWA still using name and password. I think overtime we are going to go ahead and migrate to having everybody having smart card log on but even after 4 years, I mean, it is very very few people, and people with fairly big security clearance that are accessing remotely with PKI log on.

I had a comment to that response: The PIV actually owner requires the PAV authentication key, and when you talk about log in, you are talking about the PIV key. When people talk about logical access, they really thinking secured e-mail, encryption log on, website access being able to use it securely and gone through the gate. So the comment was made earlier that there is only one required key but I do not think anybody should be considering a system that does not put for keeper and certificate signed card at first issuance or whenever you personalize.

Can we say that Judy comes back upon stage which is shortly.

Well Judy, You want Judy answer something so. What is the question you want to Judy to answer. He tried to get the answer for a little bit, the question is we want to define the difference between the local workstation access that requires two way and a password or PKI based on the risk assessment conducted for your authentication systems versus remote access and where the requirements live for PKI credential and to our logical systems. Okay the logical access that applies for local workstations which, I am not sure what the definition of that is, it could be unconnected workstations or could mean your local system that you use everyday, we are trying to find that, and then, it is best of us for level I or for use and chew it _____ password or PKI and for remote network systems that requires PKI, no matter what level, in a period. So we are trying to get a better answer as to where the line is drawn between, what the definition of local workstation is versus remote network, I mean, remote network could be VPN, that could be access in a website from a remote location.

Your getting this word local to access from where, FIPS document.

Yea, FIPS 201. Who is next. I am not the author of that and so would you write that question down and we can ask NIST what they mean by that but, let me, okay well probably.

Is that page that you guys handed me

Let me just to say about that question in general. The _____ Education guidance of Federal Agencies which is OMB MO404 defines the four levels of assurance on the application side to determining what your level of risk in your impacts and therefore what level of assurance you need. Right and then this 800-63 tells you the technology solution that make that level of risk, okay, so whether it is a local workstation either connected or unconnected from a network or a remote workstation you should be doing remote access, you should be doing the same kind of risk assessment and determining your level of assurance. Now, I do know that the folks at _____ going to go back to 800-63 because PIV was not around when the rode a 800-63 and so they are going to take another look at 800-63 and actually work in where PIV card that is being accessed with the password versus a PIV card is being accessed with PKI whatever you turned on and what pieces of your access fall at what levels of assurance because we may think pin password in the purest sense, we are actually thinking just pin password and what we are dealing where there is pin password that works with hardware token which is something I have and something I know which is two factor dedication which might just be something other than what just the password by itself would be according to 04-04, so that is something that is still being reviewed by the computer security division and I will find out where they are with that, but as far as defining local terminal etc, etc, I think that is upto your agency, that is an access piece versus a remote workstation.

We will take the question to NIST instead of pursuing it ad nauseum today because we need to move on. Thank you very much. If you have follow-ons to that, I am going cut this off now because we do have too much of an agenda for the small agency group meeting that we want to get right into show. If you would just a round of applause for the folks appear who had been the victim.