Industry organization dedicated to smart cards as we come to a smart card solution called the smart card alliance. The leader of the organization is a very kind guy named Randy Vanderhoof, who has spend a considerable amount of time with us for the last 3 years at the project managers groups on a regular basis and just putting together technical groups as we have two technical groups under the response 2, I think may be 3, but I am thinking that FEPS 140 technical group that is doing a lot of work right now and there is some other papers that Randy may or may not talk about that on the website as well that are excellent references for those who may be getting started one amd want to know what is this all about. We, as the IAB offered our members that use that site on a regular basis that those resources are fully supportable to us and some of our peers and in fact one of my transportation colleagues is actually chairing the transportation council for the smart card alliance so without further ado, the chairman of the smart card Alliance Randy Vanderhoof.

Randy: Thank you very much, Jim. This has been really an interesting opportunity for me to represent the smart card industry in this entire process of the HSPD 12 understanding and implementation discussion that we have started here today and I know is going to continue on much longer than this individual workshop, but we were putting together the agenda for this event, we in the technology side always like to jump in and start talking about the technology, the cards and readers in the software and what it does and how it works and all the security features and such but we really had to tailor that enthusiasm towards you the audience who are the government implementers and users of this technology and back away a little bit and not talk about the technology as much as talk about the process, talk about the business policies, the rules, the implementation issues, because until you have a firm understanding of what is in front of you in that aspect of it. You are waisting your time, starting to delve into the weeds and getting into specifics about cards and leaders in software and security features and such, so what we are going to do in this session is we are going to talk about the implementation issues from a perspective of what are the various components that are going to get discussed at a much detailed level once you get into the actual physical implementation of your PIV cards and applications for those cards and physical access and logical access ajd such, but today in the interest of maintaining a government to government dialog, we are going to have again our experienced folks from the IAB who have been implementing smart cards who have the learned the hard way, who have worked diligently with industry to get us to get our act together to make sure that the next stage in this implementation runs much smoother than what they had to experience in terms of going through the bumps and bruises of getting the programs under way, so we are going to just take the hour session here and go around to these various speakers here on the panel and talk about some of the top end components of what we are discussing in terms of a secure identity credentialing system specifically the card design issues and stock issue, the card issueance software and use of the software for provisioning and getting cards out into your agency population. Some of the printing options that some of these people may have had to deal with in terms of centralized printing verus decentralized and how do we get throughput of cards through our systems and out into the population, the distribution issues, we have agencies here that have clientelle all over the world and distribution is going to be different for every agency and many of you are going to have atypical models for how you are going to get your cards issued and out to your population and then slightly may be we can talk a little bit about the card management issues in terms of thinking ahead about what we are going to have to deal with when we have turn over in our personal, when we have changes that have to be made to our system and we have to go back to our initial credential and do something with it. Are we prepared and what decisions

should be thinking of now in anticipation of those times when card management issues are going to become a real issue for us and then if we have time I would also like to have them comment on some of the application view points of using the smart card credential in the area of door access, mobile security access or logical access implementations.

So with that as the framework may be we can start and Tim if you would not mind sharing with the groups some of the issues that you faced in NASA as you were planning out your overall infrastructure relative to some of the decision points on the component levels of the PIV.

Tim: We got involved in fairly significant ways that Mike acknowledges earlier, thank you, for the work involved in writing the technical implementation guidance for smart card enabled physical access control systems. So we called that document the TIG, for short, so I won't say that long name again. We basically approved this document through the IB in the FICC process last summer about a month before the HSPD 12 came out so we had spent outside probably 12 to 15 months looking how to work with smart card based physical access control systems and the technology was new. There has been, I think ongoing debate in industry is to whether or not you call smart card RFID. I think the critics claims, you only probably have to say that is RFID plus something because if you tried to discedit the claim of RFID you can say it is radiofrequency and it is an ID so what is the problem here. So I think that has been an issue that has gotten a lot of press. What we need to look at though is how much different this smart card access in the reader environment is from what you might use of packaging and again one of the principle differences is the technology, if it is a proximity card or proximity technology versus a vicinity technology, which is what typically RFID is. The importance difference there is you are taking about 5 cms versus 5 meters and you are not trying to track luggage or boxes through handling equipment. So you look at a number of security questions around contact-less cards. I am sure that you can find reasons and challenges against using a contact was smart card in the manner they we are taking about compared to say a bar code or a magstripe because you know, bar code or magstripe if it is in your pocket, you obviously cannot read it and if it is a magstripe, if you do not swipe it obviously you can not read it. So there are some different attack vectors, so the approach that we took when we wrote the TIG was we are going to add some additional things to the card to ensure the data integrity, the numbering scheme that we have talked about a little bit, the FASC federal agencies smart credential number that is contained in the card holder unique ID, which has now also an expiratio date, which is a FIPS 201 enhancement, those are all consistent with a very very wide industry vetting as to how to implement a contact-less smart card solution for physical access control. Now having said all of that, we are really still talking about the front side of the card to the reader and how that reader connects into your existing infracture was left at the discretion of the reader vender so that you could have interoperability amongst existing PACS, physical access control systems, so that you do not have to go and do system wide replacement. There are other issues around that I think you should look at deployments as to how you are going to maintain physical readers when the typical infrastructure is a one way communication from the reader back into the panel and the other control parts of the systems where if you have like the computer you can do bi-directional and send updates down to the readers. Most fo the reader vendors I have talked to you that have these solutions have ways to update the readers without unscrewing them from the wall, which means that they have got some other built in security features.

Its sort of a high level overview of the readers and the card interface. I have a tendency to get in to a lot of the nuts and bolts and then I want to try to keep that high levels.

Tim. if I could just may be direct a question to you relative to the decisions you made in terms of card issuance, modes, have you approached that based on your agency requirements and how that was implemented.

Tim: So, here I guese is the skinny as they would say, we have not deployed a contact-less smart card or contact-less smart card readers yet because we are waiting for the dust to settle and we do have product in hand that has been provided to us that will support this although I will not assert that we completed appropriate testing to prove that everything is to our satisfaction. I think we are at the very point of being able to say that we have got cards that we can independently encode and test on multiple vendor's readers but we have yet to do that. So in the meantime, we are doing what I think although the largest percentage of prox card instalations do now and are using 125 KHz or possibly Mifair or other similar technology. I think Cubic has one too. They are proprietary, they are not iner-operable but the infrastructure upgrades that we have been putting in place over the past several months will support whatever reader that we select and so our approach has been to building infrastructure that we know and understand and prepare to accept the technology when it's been fully certified and accredited. So we are not prepared to make the deep investment until we see these in multiple implementations, which in a way would make a defacto CNA, but we are hoping that the documentation that it has been discussed today will come forward and provide us an accredited vendor list.

Thank you.

Kevin.

From the DHS perspective, we were able to, and have deployed, a small implementation at the headquarters level. We did issue the cards on site, our future plan is to of course have both capabilities to issue cards on site and to hopefully leverage card production center in Corbin to really push out cards we have to en- mass. So those are things that we are looking at as far as leveraging our internal resources. We do use our cards today for both physical and Cyber access. We do have readers on the doors that are both biometric and pin and proximity readers, of course we use contact-less side for our physical access and he contact side for logical access. We have biometic keyboards that are workstations that we use the cards for, so we are leveraging both those technologies and Tim alluded to they are obviously somewhat proprietary just because of the nature of the standards that do exist but really have not been implemented government wide. We certainly have leveraged our PKI infrastructure that we inherited from Legacy INS and have pulled that in to the mix as well, which has been just recently cross- certified through the federal bridge. So we were able to leverage that technology as well, which enables us not to have to reach out to the share service providers but to use our internal solution to provide the PKI. Along those lines we are also, the biggest use for us is the infrastructure and not having to create a separate infrastructure to support the smart cards as the DHS rolls out its enterprise architecture which I have talked already. We plan to use that in concert with our PKI and our smart card technologies to make sure that the cards get out and access is established throughout DHS. One point, I want to make is to further articulate the difference between what the cards we intended to do and what the reliant parties are intended to do. The card and the vetting rocess and all that that

binds the person to the card itself is more for authentication and validation of the person. Just because I have a smart card it does not mean that I now have access to every day just facility. The reliant party either your building management or whoever that will be or your CIO shop on the Cyber side,

The Department of those folks still have control of what systems and/or facilities you are able to access. The card is merely a platform to allow the reliant party to manage those assets and those accesses. Obviously, as we begin to scale within DHS trying to figure out what the best way to get cards out to the various components, we are looking at least in the near term to work with FEMA to possibly create our enrollment stations that we can both leverage that way creating more like generic work stations and enrollment stations that any DHS employee could come and enroll in and that is kind of our vision. Since we actually have a lot of the answers to a lot of the questions, we want to just be able to just create those enrollment stations in that environment a single time and then leverage it throughout DHS. So, that is kind of our overall strategy and I see we have some fairly aggressive timelines to make that happen. So, we are working furiously to make that happen. Thank you Kevin. Michael.

At the Department of State, we have been issuing cards, smart cards now for approximately two years, but going back before we began our program, we have had an antiquated access control system in place and it was decided that that needed to be replaced. As such, we look at the technology that was out there at that time and I'm oing back now to 1996 when this was been evaluated, it was determined that smart card was probably the technology to go with and at that time, contact was primarily the only form, contactless was being talked about. There was some _____, but nothing was really available for massive issuance. So, we began with a renovation of our access control system. Now, what that entailed was not only changing readers, we had to change complete infrastructure, the whole head and system had to be replaced. So, all of our servers that had to be changed out, all of the software was changed out, all of the wiring had to be replaced, in fact, was still in the process, and all of our panels had to be replaced. As I said, we are going from a old wiggin wire, which is a one-way communication system to working towards 485 dual-interface communications process. So, we have to think hard of the expenditure and what we wanted to do and since smart card was decided, that was the way to go. We committed ourselves to that and it is a major upgrade of our infrastructure. This is something that once you get started in a lot of cases you don't realize the involvement of what's there, what you have to replace. Some of the things go back, you know, 30 years and when you start pulling wiring, you realize, you just can't pull out this wire and put in a new wire, you might have to run all new conduit or you have to drill holes in floors and walls. So, it's a major undertaking to actually replace your infrastructure and that was one thing that really surprised us, the complexity of it. Once we started and we started to put in the contact readers at our parimeters at the beginning one of our concerns and everyone expressed that we would have problems with the backlog of people coming in and out of, we have turnstiles at with most of our parameters facilities, that just taking our headquarters the Harry S Truman building, there is approximately six thousand to eight thousand people working there at any one day and when you look at about 07:30 to 08:30 or 9 o'clock in the morning, you are going to have to bring all of those people in and we expected a lot of problems using the contact card to get in and out of the facility. To our surprise, there wasn't the backlog we were anticipating. There wasn't the complaints we are anticipating. This is not a metro where people are literally running to get somewhere to there, they are coming to work, right? Some of them right. So, with that were quite surprised that the

infrastructure we are putting in place, the contact card was slowing down the entry by approximately two seconds total. That's not a lot when you just sit there and start to count 1000 and 1001 but when you are standing at a turnstile and you got your card in the reader you know something is got to happen. I do not like to stand there and wait. That 2 second wait can be like an eternity, but we did not get complaints and the arguments, again, that we had originally anticipated it so. We were kind of fortunate that way, We still have a lot of building to do to replace the infrastructure. We got 44 annexes in the National capital region, which we've got at the convert. As I said earlier we were about 80% done with our headquarters and we have got 13 of our annexes done of the 44. Again this is not just replacing readers. It is not just going up the wall and taking off the reader and putting on a new one. There is involved. Choosing the reader -- what you got to look at is when you buy a reader no matter what vendor it might be you have got to anticipate that another vendor's reader may have to go in that location some day due to a competitive buying. You can't sole source all your life. You got to be have that capability of replacing one vendor's reader with another so make sure that how you build your infrastructure it will accommodate multiple vendor readers. Make sure that your back end system, the head end system will accommodate any changes that we might be able to make easily. So there is a lot when you are looking into putting in or replacing the system. It is expensive. If you think this is going to be cheap, if you have got a system, an antiquated system, or you are going to put in a brand new system, there is a major expense involved. These products are not cheap. When you are installing, let's say a new software, make sure you get the latest and greatest but make sure that it conforms to your needs, make sure that you write in your contract that any upgrades are available that you don't have to pay an outrageous price for another upgrade. There is a lot of planning that has to take place in order to put in a new access control system and a smart card is just one aspect of that technology. So think hard when you do it, but don't be frightened off. It is paying off for the department of state. It is moving forward. We had a little rough point at the beginning, but we were one of the first few agencies out here putting in a new smart card physical access. So there was a lot of lessons learned. As some of my colleagues would say, if we can go back in time knowing what we know today we would have done a lot of things differently. We tried a mass badging effort. We decided that in order to do the Washington the capital region we would need to swap out or at least issue new cards to approximately 20-25,000 people that work right in the Washington capital region here and we felt that a mass badging effort pulling everyone in to certain points and taking new pictures and enrolling them into the new system and issuing the new badge would be easy but it was not. It wasn't easy. This is something again. It is one of those lessons learned, you learn in the hard way. We have done a advertisement campaign if you would put it that way. On our Intranet we advertise we put commercials that on what we call our B-net it is a televised network within the state department, telling about our new smart card program. We took fliers out. We slap information stickers around every elevator to get people to come in and get their cards and it is a culture you have to break into. A lot of people said, well I work out at annex A so I am not going to need that card because I don't come into a headquarters, but once in a blue moon. So they are not get their card until they absolutely have to. These were issues we did not expect that type of resistance right up front. We thought there would be some, but I think it was more than what we anticipated. Then you have got the hierarchy, you have got the assistant secretaries and under secretaries, well they are a little bit above the average workforce and why should they come down again and get their card, can't they send their secretary down you got your old picture and you know the process is changing now with the new PD and the FIPS. There is politics that you have to look at

also, so it was a very exciting in one way a lessons learned and we are glad to share some of that. As I said one of my presentations at one of the conferences even punching holes in the card so we can put a little chain around there. Well since it was a contact card

No contact lists anywhere we did not worry about an antenna. Well, now we found out that after we laminated the card we punched the hole and now the laminates starting to peel off. Well, this is another thing, did we punch the card the wrong way or little things like this that pop up afterwards. Damaged cards, we did not expect that we were going to have such a high ratio of damaged cards. People do not take care of the cards. It is not so much that they are willingly damaging the cards, they are just not paying attention, even though we send as much information as we could how to handle your card. One of the problems we had on readers and I am going to throw this out because it cost us- a lot in one respect. The old Reagan card that we have here is about may be a 100 mils thick and the new smart card is 30 mils thick. It took a large campaign to educate the employees plus we worked with our vendors to try to correct the problems. People would take their old card and jam it into the reader. The reader was not designed to accept the 100 mil card and it would bust the contacts inside. At the same time, we see people taking the new smart card and swiping it in the old Reagan reader. So, that it did not hurt the card, but the old card being stuck into the new reader did cause us a lot of problems. That is the lesson learned that it cost us dearly. So, there is a lot of things when you are implementing a new system what you should look for? what you may not think about up front, but it will happen to you? Thank you.

Now, we did not actually plan this to have that two guys over there that have not actually issued the cards with their rosy projections of what they are going to do and then Mike over here who has actually been through the wars of reissuing cards having a slightly different perspective, but it is turning out that way, but one observation I would like this to make though behalf of Mike is that I have known him since before he started issuing these new cards and I think he looks 10 years younger than he did back then so, it is definitely a rejuvenating experience and I would encourage all of you to look forward to that as an opportunity in part of this process.

No Randy, he decided when he is retiring, that’s all that is.

So, Jim Zack, what words of wisdom that you have for us.

Jim: The devil's advocat gets to speak so here we go at the end of the day. Some of this would be recap of lot of things you heard earlier today. My role with your organization has been devils advocate for about three years now and I am like "why are we doing this? how is this going to work? and some of the things you have heard throughout the day today, I want to hit them because Randy hit the key words and I want to spend a few seconds on some of these things and if it makes sense cool, if it does not make sense, ask me later and I will tell you why I did not translate it well up here. The first generality is not one size fits all. We have talked about generic solutions all day long and the truth of the matter is as we have gone through and developed each of the documents that have been talked about today. There have constantly being questions from folks "well though I have to put a reader on every door?. No, What do I do for store fronts verses headquarters, what do I do for regions versus headquarters, what is my infrastructure? what am I going to do with another agency? We touched on some of those things all today, but now you have an implementation plan that is due very very shortly. If you want to backup the due date, some of the decisions I am going to talk about in the next five

minutes, you should have already made them. If you have not made them, you best go get your teams together and make some decisions pronto or you will not be able to fill in this guidance for your department or your agency. Things like, what is my business process going to be? and where am I going to do things?, how am I going to do things in each place, when am I going to do them, how are those things going to be hooked up to one another? We have alluded to those things. Guys, it is a killer because when you do not think them through and when you do them wrong, retrofitting or fixing those things is extremely expensive. Mike alluded to some of that and the lessons learned. Kevins alluded to a few things and Kim, God bless him, has given us lots of things not only today, but in past days. So, you have to do some risk assessment for your systems, for your physical infrastructure, where am I going to apply this stuff, what am I going to apply, which ones do I do first, and will that satisfy the control objectives now, and will it get me into a logical migratin path next year.

First and foremost you got a self-certification responsibility that had got to come up this year. Who is doing that? Do not trust your IG to do that for you. I think for most of agency meetings I have been, including our own, when the question came up well, who will bring the IG in. Most IGs from past experience would say, you make the decision, you make the call and I will tell you whether we like the call. Do not anticipate this being any different in that regard. So they may come to your meetings, they may nod, may nod their head up and down like this, and they make some faces, but once you implement they will come out and say, hmm, that plan is not working very well. They are auditors, that is what they are paid to do. They are not paid to implement. So, the burden is on you, you have go do it. You have to figure out the self certification. You have to figure out what the applications for this stuff are going to be in this stuff. Now, what we talked abouttoday is some of this stuff is going to get easier for you over the next two years because tomorrow you will hear a little bit more about the conformance testing and the fact that we intend to, and Judy alluded to it in her presentation a little earlier today, that we have been beating up on NIST for the better part of two years about making sure that the general programming and applications fit. That the readers work together, that we can certify products beforehand, that when we plug and play. as Michael said, you are not going to get the same one all the time. Things happen. You have to know when you plug and play for equipment because that one is not available today , the vendor cannot ship to you because they have an order for agency B Well, that is going to pop up, don't you think? So, you need to figure out how you are going to get into the mechanism and pay attention to those things now, not after you said okay, here is my plan, I'm going to implement my plan and I have done a purchase order. "Whatever will go wrong, if you are coming out of the gate, probably you will" is what everyone has said to you at some point today and the choices that you think are optimal today may not be optimal six months from now or eighteen months from now and frankly you are looking here at least four to six year life cycle of what you are going to be spending your money and your time and doing your documentation on. This is a big IT, a big personnel process, a big huge to-do and when we talked about the contractor data before, that is a new role for all of us because one of the things we have learned when we negotiate things, when we start talking about border management, we start talking about things with our colleagues overseas and Michael knows this better than most of us. What do you trust? Which process do you trust? A few years ago we did a process where we had all the transportation modes and it was said let us talk about cross-vetting One particular mode of transportation, in fact, looked up us and said not in this lifetime. Not with us, because if you come in our space, (it's the railroads), if you come in our space we will do our own. Again, we have a

couple of folks that we want to partner with that some of us in the room have partnered with and are partnering with, who have fundamentally say that's nice, but that does not get it. We have heard about Indian Affairs that is nice but we have something in addition. We have got some state laws in there depending on where you are and who are going to partner with that will also come into the process. Some of these state laws are different than the federal laws. So, if you have things in state's face that will bite you if you have not investigated it. So, homework up front, think about the infrastructure, think about the risk management that you need to do, both physical and logical access and deal with what you need to deal with most importantly. You have got partners you want to bring in whether it is contractors. One of the things we have not succeeded in figuring out yet. I have a contractor that I am vetting in my department because they are there. They are basically resident. If they lose that contract for some reason and they go to work in another agency. Have we thought about how we are going to move the contractor data? We have enough trouble thinking of how we are going to do the employee data and the employee vetting and now we got the contractor vetting we've got to add to the mix and we do not have a lot of time to do that. So, this is just a way to say, come up with more questions, we have a lot of work to do, individually and collectively and that for now will cover it for me. Thank you.

We are going to open it up for some questions now, but I think what I just heard from four different perspectives here just gave me anb idea of kind of putting in perspective. If you think of what it is like trying to put together one of those 1000 piece jigsaw puzzles and you open the box and you dump all the pieces out and spread all over the table and you go, how is all this going to fit? I do not even know to where to start. There is just too many open questions. This is impossible, never going to happen. The way I was taught to start a jig saw puzzle is to start with the outer frame, right, the things that are the easiest to identify, the things that are going to create the frame work for how you are going to build towards the completion of that and if we look at these change processes and we look at the these decision points that Jim talked about, we are really talking about the frame work and then as we get in to the practical implementation within your particular agency the decision points that you are going to make, they are going to be those small pieces that are going to have to get fit together uniquely for the way your agency is set up to operate. So maybe that might help in terms of framing this. Question?

Ron Martin from the Department of Commerce. There is a couple of contract vehicles that one can use to purchase whatever it is that we are going to have to buy. I know we have the smart card GWAC the Government Wide Acquisition Contracts. They also have the schedule 84, which you can buy security equipment of course, you can go out and bid your own. As we go through this process some of you have been through portions of this. We should be using the GSA contract vehicles to the greatest extent possible. I mean what is your recommendation on how to, since we are not in the smart card business today and we have to go there. So what is your sense on, where do you begin, GWAC, schedule 84, IT people wants schedule 70, all of the above, none of above.

We use, for our smart cards, we use the GWAC. That doesn't say we will continue with it. As Mike Butler said they are rewriting a lot of the procurement. DOD is trying to put together this aggregate buy and I heard Judy saying that they are going to try to get some more vendors on the GSA schedule that could offer some products and services. You will have to really evaluate what your needs will be. If it is just for smart cards, if it is for readers. I can't tell you where you should go, but we did go with the GWAC for the smart

cards. That at least referenced, in part, some of the standards that you will need.

Tim: We issued a task order request through the GWAC, it has been about two years ago and we went through the whole bidding process which at that point in time you, we found ourselves in a first. The best advice that I have been given is not to be the zebra on the outside. We found ourselves on the outside a few times here. It presents some risks that I think you have to live with and in terms of being at the front of the pack and we have tried to follow pretty much in close proximity to what DoD has done and not get out in front of their work because they just have so much momentum in the market and driving what has been practically developed through experience. The best guidance I can give from that is that we have watched what DoD has been doing using the GWAC to get there, that is the formula. I think just one thing to take note of his as Judy alluded to, as you look down and started pull the implementation plan together for everyone to use as a kind of the recipe for that. We did look at what type of equipment and services we would have, people have to purchase to try and pull this off and I think that plan is going to walk us down a new path which will create some vehicles for purchasing readers and purchasing security equipment which traditionally would not have been involved in these smart buys. So I think as we put the plan together and looked at what traditionally will we have to buy that is outside of these traditional aggregate buys that we originally had and you will see some of those things come forward. It certainly will not be in the near term all though, you know it is kind of a collaboration through ourselves and industry and the vendor community, but I think that we are heading down that path where most of these products are going to be able to purchase and services from an aggregate buy.

Hi, Karen Erikson from Department of Veterans Affairs. Couple of comments. First of all to my colleagues here, I would like to encourage all of you in your response to the draft guidance to strongly express your opinion regarding the NAC. That the NAC should be replaced with something less stringent such as fingerprint only. Certainly supporting HSPD that we have a higher level of security and that type of thing but I heard a lot of comments here today about people concerned about that as the minimum type of investigation. So if I could do that, but to the individuals who put this on today with lot of discussions also about the need for collaboration and the willingness to collaborate and I think that is great but have not heard a lot of contact information nd I do not know if that is going to beyond the NIST website or where that is so that we know who to go to and how to contact people so I have not heard that yet.

Two places, John Moore's smart gov site has a project managers web listed on it and all the project mangers are on there and those are decent contacts to start from. That’s a good place. The other thing you will have is you got the speakers here John will put the e-mails of the speakers on the notes on the web and because on the Q & A etc. At the end of the day you will have the contacts. It is smart.gov

That would be preferable rather than having us key in the questions there and we will key the ones we've got, but it will be there on smart.gov. Yes, by the way one of the frequent questions here was what about soft copy on the slides, which they will be there by Monday. All of the presentations plus the telecast that we are filming.

For all those that are still on the phone, for your questions go to smart.gov so that we can handle those. Everything we have covered today, everything we will cover tomorrow will at some point, go on the smart.gov website, and it

will be available by the first part in next week and hopefully including the tape and the movies so all of our less than apealing faces are there for you see, and if you asked a question you are not sure about, you can go see it again and see if you really want to ask it and judge for yourself from your desk.

I just come in on a couple of things that you brought up. The whole issue around the NAC. The NAC was highly contentious and obviously everyone weighed in for and against and made their positions very clear, but at the day the comprise was that you know you need to have the NAC with the inquiries in progress. The initial thing was to have the NACI completed before you move forward. Now that will effect different agencies in different ways if that is part of your process now. If you have built in that time in your current bidding process then it is not an issue for you. You already have built in the time for that process. (pause) Mike we got a ton of public comments on that.

Just a quick addendum to what Jim said regarding websites. Since this is not just about smart cards, it is about smart cards and PKI and biometrics, you also need to take a look at the FIC and the federal PKI websites for information on those particular technologies. (pause)

While we are doing that of course Kurt talked about it. Tim talked about it this morning. The most frequently asked questions you have which we did not go through today because I dry-ran that with the an agency last week and it took me an hour and quarter to get through 25 questions, and they all had this Oh look on their face during most of that discussion, but those questions are on the NIST website if you just popped on NIST and popped up PIV and its computer security division, you can get all the publications downloaded. You can get all the questions downloaded. It is a wonderful resource and, as Kurt said, they are expanding that to include the links to these other sites as well, so ignorance of what is going on is no excuses it is just overwhelming to keep up with all this because it is several hundred pages.

Jim and John, I was in here early in the morning when Judy was speaking, but did she talk about the Federal identify handbook.

So on the agenda for tomorrow it is the last two sessions.

I just want to touch on that in case if there was any of you here they are not going to be able to be back tomorrow. The Federal identity management handbook is a very detailed description of this entire PIV and PIV implementation process and it is a great resource for you. We are going to actually go into some of the details that are in that handbook in tomorrow’s agenda, but you can access that handbook from our website, the smart card alliance.org website or from the smart.gov website or the FIC website on that.

For that Ralph gets to do a 30 seconds commercial since Ralph has done a lot of the heavy lifting for Judy on putting this handbook together. We are going to talk about it a lot tomorrow afternoon, but Ralph, if you would, just a website, post things etc.

The handbook is available on a number of web sites, but the one I most familiar with this is cio.gov/ficc so it is available there. We are going to walk through the highlights of the handbook tomorrow in the afternoon.

More questions?

You want to do the preview for tomorrow.

I want thank the panel for being up here again, long day.

As always thanks to my friend Randy and listen before you go thank you very much for your time and energy and patience. This is important to all of us. We only get one shot at doing it and if we do it badly we woe be to us from the OMB and the congressional perspective. Tomorrow we are starting here at 8:45. We are having a new whipping boy tomorrow morning Jim Dray of NIST will be with us in morning, and Jim, as most of you probably know, is largely responsible for the contents of special pub 873 which is the technical implementations, so come armed, even do a little pre-reading tonight so, you are really loaded with good questions for him. Go forth and This has er quoth Spock. We will also have folks tomorrow. Judy will be back to talk about some things and it will be a lot more ont the technical guidance, technical issues of this.

John you had to closing comment. John: Yeah,

Closing comment -- several people may be leaving tomorrow, may have large luggage, so see me and I will provide a storage room for that on the second floor. Thank you all very much. Good evening.

You all know what it takes to get back in. We will hope to have that much better organized tomorrow morning.