"U.S. Department of Homeland Security
First Responders Card Initiative"

Wednesday, October 26, 2005
2:30 p.m. – 3:30 p.m.

All Hazards Forum Conference and Exhibition
Baltimore, Maryland, USA.

Moderator:

Craig A. Wilson, First Responder Partnership Coordination, Office of National Capital Region Coordination, Department of Homeland Security

Scheduled panelists:

Anthony M. Cieri, Senior Consultant to the Department of Interior and Federal Interagency Advisory Board

Lemar Jones, Jr., Director, Antiterrorism/Force Protection Directorate, Pentagon Force Protection Agency

Mike McAllister, Deputy State Director, Security and Emergency Management, Virginia Department of Transportation

Brad Jewitt, Director, Office of the Fleet, Facilities and Administrative Services, Maryland Department of Transportation

Jack Markey, Director of Emergency Management for Frederick County, Maryland

Elmer T. Carreno, M.D., Deputy Health Officer, Prince George's County, Maryland

Chris Tonjes, Director of Special Projects, Office of the Chief Technology Officer, District of Columbia

Transcript of session:

MR. WILSON: The National Capital Region First Responder Partnership Initiative will provide federal, state, and local first responders with public key infrastructure certificate-based identity smart cards that will enable their identity and emergency attribute to be electronically verified during a crisis incident in a communication in or a communication out environment.

This partnership is leveraging the technical requirements as defined in the National Institute of Standards and Technology Federal Information Processing Standard 201, more commonly referred to as FIPS 201.

It is also leveraging FIPS 201 in General Services Administration's federal certificate authority to issue PKI digital certificates to the National Capital Region first responder community based on minimum levels of identity requirements.

This partnership will be scalable, in support of the National Incident Management System, and the National Response Plan.

The panel consists of partnership members representing federal, state, regional, and local

leadership. In particular, we have Anthony Cieri right here, who is the Senior Consultant to the Department of Interior and to the Federal Interagency Advisory Board, and Tony will give a fifteen minute overview of the partnership.

And then following him will be Lemar Jones, who was the Director of the Antiterrorism Force Protection Directorate, Pentagon Force Protection Agency. Lemar will talk about his 9/11 experience. He will talk about what PFPA -- that's short for "Pentagon Force Protection Agency" -- PFPA has four million CACs out there and how he's leveraging the opportunity to use those CACs to build the business roles for the handhelds that I'll show you in a few minutes.

And beside him we have Mike McAllister, who is the Deputy State Director for the Security and Emergency Management for the Virginia Department of Transportation (VDOT). Mike will talk about his 9/11 experience, the Governor's endorsement of this initiative with VDOT as the lead for the State of Virginia, and the applications that he's looking to develop for transportation.

Beside him is Brad Jewitt, who's the Director of the Office of the Fleet, Facilities and Administrative

Services for the Maryland Department of Transportation (MDOT). Brad will talk about the Maryland Governor's endorsement with MDOT as the lead, and MDOT usage for force facilities, their headquarters, et cetera, et cetera.

Beside him is Jack Markey. Jack is the Director of the Emergency Management Agency for Frederick County, Maryland, and Jack, because of his location, will talk about things that he's been involved with respect to the No Fly Zone violations. For those who read about them in the paper, well, he's the man that had to coordinate all that.

And also he ties to [inaudible] and his emergency response caters to Fort Dietrich.

Beside him is Chris Tonjes, who's the Director of Special Projects for the District of Columbia and the Office of Chief Technology Officer, and Chris will talk about DC's endorsement for one card to model the federal government and potential application of element.

Before I go further, I want to show you that one of the things that we're getting towards is being able to not just issue cards. That's not the end state. The end state is to be able to use the cards for emergency management so that you can identify your assets and quickly define who your human resources assets are, and what we're

looking at is to be able to put the PKI solution in a handheld like this so that you, in fact, can show red, green, or yellow, depending on whether somebody meets the quals, doesn't meet the quals, they have the right privileges, et cetera, et cetera.

So having said that, I'll turn this over to Tony Cieri. Tony?

MR. CIERI: I'm going to breeze through this. I'm going to talk to you a little bit about technology. This isn't about technology applied. I'll tell you what the technology does.

I think that the heart of this will be in the users. What you see in the users is a wide diversity of a community from Virginia to Maryland inside the NCR (National Capital Region), the DC government, from inside the NCR and outside the NCR, and how we can have all those multi-jurisdictions trust in an identity across all those different jurisdictions and add something which I'll refer to as an attribute attached to that, and that's what we're about to demonstrate in the National Capital Region with exercises next year.

[TO MR. WILSON:] So if I can have your glasses so I can see this? Not only is senility setting in, but so is

age.

What's the requirement, where did it come from? What are we leveraging? What's the population? solution? What's the technical requirement? What does it do for an incident scene commander, and how interoperable is it? Hopefully at the end of that we'll have answered at least some of that.

So pick and choose. I'll pick track demand. What do each of these incidents have in common? Could you get across the multiple jurisdictions with an identity card?

I'm going to stop and say, forget the word "card." I've got up in four forums in the last three weeks talking about the word card. This is not a card. It's a technology platform that you build off of. That's what we're doing in the federal agency side. That's what we're leveraging right here. That is what FIPS 201 is all about.

It's broken down into two pieces. Identity vetting is the claimed identity, the real identity, and can you prove it? And secondly there's a technology that corresponds to that that is issued in a very secure way. We're leveraging that off the federal side for a much larger population to include not only the federal agencies,

but include all the state and local jurisdictions.

Some of you may have heard of HSPD 12. If you haven't, go to Google. After you go to . . [http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html]

With that all said, FIPS 201 draws a line in the sand for the first time ever globally on identity and how you go through technology with identity. It starts with identity vetting. It ends with a whole series of documents which involves a smart card and PKI and biometrics.

We're moving to three factor authentication. It is intended for the executive branch of the US government. That's the intent. Having worked with Tom Lockwood for the last thirteen months, I truly understand that I flunked civics because at the end of the day the federal government can't tell the people that I'm looking at what to do. They can't even tell the legislative and judicial branch what to do. But the judicial and legislative branch sees the value in doing this, and they will also proceed.

This is leveraging what the Fed is in process of, starting with tomorrow, by the way. . . .

What are we trying to do? Here's a perimeter. I don't care if this is around the Pentagon, Crystal City

(Virginia), Manhattan, or around the whole National Capital Region. How do we trust identities into, out of, and within an incident area?

I think Lemar is going to speak to what happened in 9/11. Mike is going to talk about the traffic center across the street from the Naval Annex and what that assignment was and how identities are important to these very things.

So let me just leave you with identity is the cornerstone. It's the cornerstone for every behavioral transaction. Yet we treat it as though it is commonplace, every behavioral transaction you conduct, every place, everywhere, any time, and how do we trust that identity?

Just think of the multiplicity of cards that you carry around to prove you are who you say you are. How can that be trusted outside of that environment? How do they know it wasn't forged? How do they know it wasn't counterfeit?

In doing this, we started to look at what is -- This all started with COOP (continuity of operations) and COG (continuity of government). But as you start to define the population, you start to define the population at a much larger community. In the federal space, all the

federal agencies will be issued this type of identity card, a chip card with PKI with the platform available to be loaded with biometrics later. But also in the state communities there is already penetration.

The National Guard already have CAC cards. The Coast Guard already have CAC cards.

So the penetration is moving outside of places like Iraq to within the country, and that's the leverage. How do we leverage that to a whole other segment of the community? How do we control well-intentioned people like volunteers that when they come to a space and offer their services, like moving down towards Katrina and not being utilized because they cannot be trusted, and where is the accountability for that?

This is set upon as a different strategy. It's very akin to what we had done in DOD, but it leaves the identity to the identity source, meaning each of the local communities, each of the state communities, each of the federal communities. It doesn't matter. It's just a set of rules put in place by a standard. You follow the rules. You issue this type of credential. You notice I didn't say card.

Every night when you do the PKI, every 24 hours

you have to issue a revocation list. That revocation list is seen by that thing in the middle called a validation authority and also that attribute authority. It's basically two separate functions shown as two servers. They're really one server.

The issuer determines who has been sponsored to get a card. What is the identity? What is the identity vetting that they have done prior to the issuance of the card?

Those servers hold nothing, no identity information at all. They're very akin to what happens when you conduct a financial transaction; numbers only encrypted in a sense that there's very, very little information about any identity, with those servers talking out over a GPRS link nightly, within 24 hours, or sooner if you want, after those handhelds that Craig's going to demonstrate to you very shortly.

So this isn't a concept. This is real. It just leverages a $2 billion investment that already was done on the federal side.

It is not painting the world purple. It is standards based. So if you're a vendor here and say, I have a better solution, cut me a break.

The concept is for the people to be pre-credentialed or credentialed on-site if they haven't been given a credential, only with the same technology. They also have to be identity vetted and sponsored. After the perimeter scene is put together, they present their card to one of those relying parties who now reads the card, as Craig's going to demonstrate to you, and then makes the decision, but a much more informed decision than the flash pass, a much more trusted decision than the flash pass--something that's electrically validated every 24 hours or sooner so that a much more informed decision can be made.

Think of yourself at a border crossing point and you bringing your passport across some type of interface. You don't automatically go across. . . You're not going into the Metro [subway system for the metropolitan Washington, DC area] here. There is a decision that is made by a human before you get past the Metro. But it's only a very verified and validated decision.

It's based on criteria that've been put in place by NIST (National Institute of Standards and Technology), levels of authentication.

The last two at the bottom are what all the federal people will get. Commensurate with that will be

the identity vetting that goes along with that.

Preponderance of first responders will not have to get a NAC (National Agency Check) or NACI (National Agency Check Plus Inquiry) presented to them, but there will have to be identity vetting that's done on their side.

So let me just take a doctor, a doctor who volunteers. Is this so farfetched? What do I know that's commonplace in the country about the medical people or others, but I'll just pick on the medical. What's common is you need to apply to practice in a state. They need to go through your education and all those other pieces, and then you have to pay for the right to practice in that state.

There already is somebody that sponsors you, and there already is identity vetting. The only difference is you'll be given a credential that's commensurate to that.

The heart and soul of this is this: Identities are not taken and shipped up to some federal database. Identities are taken, secured at the source of origination in the authoritative database that already exists, and with that identity vetting and that sponsorship, are you a doctor? Are you a firefighter? Are you law enforcement? Are you, are you, are you?

After that is ascertained by the person who sponsors, the triggering action will occur to your left or to your right, infrastructure that's being stuffed within DHS. To have the issuance done at the other side of the community, not by the Fed, that's why this is called a partnership.

It works two ways. The community follows the rules. The Fed follows the rules. Good things occur.

The handheld can be programmed to do just about anything, any of these ESF (Emergency Services Functions) functions, any of the levels of authentication. It can also be used by law enforcement as a nightstick if you want to do that. Tom Lockwood likes to refer to it as "the brick." If you get hit on the head with this, it wouldn't dent my skull, and that's saying something.

Let me go back one. What am I really talking about here? Having been around DOD and the federal government for about 37 years, let me tell you. Everyone on the outside on the ring, different programs, different program managers, different money, no two of which want to talk to one another, and we worry why we don't have inner-operability. So in this case here there's a common identity framework, and you can apply it whatever way you

desire to a point where even with the state and local communities, you can even migrate this to the point as the Fed is doing so that you would have the card every day and use the card every day so that you would have it on the day.

How many times have you been issued these things and you say eighteen months later, Where is that thing?

The takeaway: We're moving to a machine-read society. If you don't want to listen to the FIPS (201 standard), read the Real ID Act. Read the voting reform that just went forward. Read what the Fed just said about two factor authentication in a financial transaction and see the trend.

It supports applications like family reunification, just for one. It's scalable, and it's a standards-based technology.

Now I'm going to turn this over to people who come from diverse worlds and how they intend to use it in the National Capital Region.

MR. JONES: As Craig said and Tony said, I'm the Director of Antiterrorism at the Pentagon, and probably, as many of you are aware, on 9/11, September 11, 2001, there was a plane that hit the Pentagon. We had several first

responders that tried to get to the building. Because of not having some type of credential that could actually show positive identification of those individuals and because of the certain threat or vulnerability that existed there--we thought there may have been follow-along ground attacks.

Our local police department stopped everyone and anyone at the (Interstate highway) 395/495 corridor, even someone carrying a badge, because as some of you may know, you can go to E-Bay and get a badge. You can come and get some of your flash and pass cards, as Tony calls them, that we use throughout the federal government, local government, and city and state.

I started in October of 2001 trying to come up with some type of identity vetting system that would allow first responders to get into the fight. They may have gone now since 2001 October.

One of the things that we do at the Pentagon since 9/11, we've issued, as Tony said, four and a half million common access cards. Every reservist, every National Guard, every contractor, every DOD civilian, every military person in DOD has a common access card.

As we speak, four and a half million numbers are loaded into this machine. Right now the Pentagon uses the

handheld at some of our over 118 delegated facilities. As many of you may know, GSA leases facilities to DOD that are not on military installations. I'm charged with protecting those installations or buildings within the civilian community.

Because of funding limitations, there's not enough electronic access control. Right now we use these as what we call random antiterrorism measures. We take them out. We post them at a building with policemen. As people come and go to work, if they're a DOD employee of any type, we insert their common access card into this and it tells us whether they're friend or foe. That's just one application that we've actually starting using just in the last month.

Another contingency that DOD actually uses this for is what we call "continuity of operations" or "continuity of government." Even though we may have been attacked on 9/11, there were still primary missions that needed to depart the area and get to other sites to carry on the mission of protecting the United States, protecting our interest.

In our current configuration, on 9/11 they were not allowed to leave because we could not again determine

whether they were friend or foe based on a visual.

What this PKI and the common access card, and what we're talking about under FIPS 201, it now allows us a public key infrastructure to positively identify the attributes that Tony showed you earlier on the handheld. Are they a part of the ESF community, and what are their roles and responsibilities as it pertains to a national emergency?

We use it right now because of the strong identity fraud, not pretty much attuned to counterfeiting, tampering, and for terrorism exploitation. That's my job. My job is to make sure that we try to the best of our ability not to have another incident as 9/11 within those 118 leased facilities within the National Capital Region.

Right now we actually just performed an exercise yesterday, actually using lessons learned, I should say, from 9/11. There were over 48 agencies yesterday participating in a tabletop exercise at the Pentagon, and I'm just going to give you a quick overview of some of them: The Department of Homeland Security; FBI (Federal Bureau of Investigation); EPA (Environmental Protection Agency); Drug Enforcement; Park Police; Virginia State; Arlington County Fire, Police, Office of Emergency

Management; Fairfax County; Prince William County.

That's just a few. They all responded to the Pentagon on 9/11.

Something that we don't make public: We had some imposters on 9/11. You put on a fire suit and you show up at a fire. Most people--most people would contend that you are a fireman. Every day right now you have people driving up and down the roads pretending to be doctors. You have people that are pretending to be lawyers. This right here, public key infrastructure, will allow you a vetting mechanism to ensure that the person that's actually standing before you is who he or she says they are.

So one of the things that we take away from my exercises now is we're onboard as a DOD entity to actually spearhead.

I'd like to invite you to an exercise that DOD is hosting with Arlington County. Right now it's tentatively scheduled for January 14. If you'd like to come down and observe, please see me after this because what we're going to do is we're going to approve the concept of our smart common access card being loaded into a database and having a full scale exercise to validate the concept.

I'd like to close by introducing Mike McAllister,

who's a part of VDOT (Virginia Department of Transportation), and will tell you how they're actually going to utilize the same types of characteristics within the Virginia Department of Transportation.

MR. McALLISTER: Thanks, everyone. I'm real happy to be here this afternoon, and I hope you feel that way at the end of this session.

How do we fit in? How does VDOT fit into this infrastructure, to this technology, to this concept? VDOT has a significant amount of critical infrastructure that set us into the Commonwealth, also set us into the nation to depend upon for their ability to travel throughout our great country.

During the aftermath, or actually on 9/11, the incident that Lemar mentioned with the aircraft impacting the Pentagon, that aircraft, in fact, flew directly over what we call our Smart Traffic Center, which is on Columbia Pike just up the hill from the Pentagon, so close that it almost clipped our communications tower.

Shortly after that, in the ensuing chaos which was started with the plane crash and other associated events, we had members of the United States military and law enforcement show up at our facility and basically

requested to use our facility as a national command post to get things back on track, and we certainly obliged them of that. So we're linked very, very closely to that tragic event, and we, too, are trying to do what we need to do to ensure that it doesn't happen again.

In VDOT we had a system that we used for security access prior to 9/11. Many of you probably use a card based system and readers on the doors, and you scan that so you can access your office or facility or something like that.

We still have that today. We've upgraded it. We've upgraded it in such a manner that it is going to be interoperable with the new system that's coming out that we're all talking about here today. So we've already found another use for this accreditation system. It just happens to enable us to enhance our security. It's a natural progression. We have leveraged everything we can on this card so that our first responders are identified properly and they can get to the scene.

We also have the ability to make sure that folks are continuing to carry this -- and I'm going to use the word "card," forgive me -- this card with them on a daily basis because they have to do that in our environment in

order to access their workspace. So we're trying to perpetuate the need to have them to have this card handy when you need it and not on your dresser in your bedroom or something like that when you're thirty miles away from home.

The other thing that we're talking about is the next step. The next step, we're not talking about January. We're not talking about later next year. As a matter of fact, we're talking about Monday. This coming Monday we will begin the deployment of this system at the Smart Traffic Center in Northern Virginia with the Department of Homeland Security working with the other gentlemen at this table.

Our facility is jointly occupied by not only VDOT representatives, but Virginia State Police. All of those folks will issue the new card so that they will be using it on a daily basis for access. It will be available to them when we have the exercise on January 14. As a matter of fact, there are some other things we will probably be doing between now and January 14 with regard to this process as well.

This is all made possible for VDOT through our close working relationship with the Governor's Office of

Commonwealth Preparedness . . . VDOT was selected . . . to become the lead agency in Virginia for migrating this concept throughout State agencies and our first responder community.

The pilot, which I said begins on Monday, will be reviewed very carefully by all of us to make sure that our processes do what they need to do so that our administration can meet the exacting standards, and I quote, standards that are required by FIPS 201. We've invested a lot of work in that, and I have every reason to believe that it's going to be successful from what I've been looking at so far.

The only other thing that I might add is if you are in the process of looking at upgrading a security access system, look very carefully so that you make the right decision because, you know, it costs an awful lot to install a security system, and you only want to do that every so often. They have a good life cycle, admittedly, but make the right choice so that it will be able to be leveraged by this particular system.

And with that, I'd like to turn it over to Brad, Brad Jewitt.

MR. JEWITT: Good afternoon. How is everyone?

We got the after lunchtime period. I see a lot of people saying this is yet another brief to go through.

Having been in your seats many times, I'll try not to rehash a lot of things that may already have been said.

I'm here to represent the Maryland Department of Transportation, our strategic partnership here, and I think the way that we began to look at our involvement was the initial penetration, and that is through the program that's looking at the NCR.

So we have Prince George's County and Montgomery County and Frederick County that play a role in that. So if we have this credentialing process that's going on in that area, why not look at how we can implement it at a strategic implementation for the entire state.

Then we began to look at what other penetration exists. Well, the National Guard has the card already, and we've got the Coast Guard, who is involved in our Port operations. We've got the TSA (U.S. Transportation Security Administration) that's involved in our airports.

As we've seen HSPD 12 and the Department of Homeland Security overseeing those agencies, it's moving in that direction. So as we examined our access control and

our credentialing process, it just seemed to make sense that we began to explore this more to see how we can build the synergy between this program and what we want to do for the citizens of Maryland and those who come through Maryland.

We're right at the brink of doing some other projects. So luckily we formed this partnership in time. Right now we have a project at the Port of Baltimore in which we're looking at our access control system, and luckily we were able to get that in the procurement process in time to look at how we can build synergies, and this is a lot of things that we want to be able to prove nationally in the rollout of this type of credentialing system.

We've got tens of thousands of personnel that would need to be credentialed in this situation.

If you think about the Port of Baltimore, you've got the personnel that work there, whether they're State employees, tenants. You've got truckers that are coming in from various sources. Think about the nightmare that we're trying to tackle here, but we're willing to do it because it's the right thing to do, and we think we've found the right solution to do it. But ID vetting is going to be very important.

You've got foreign nationals that come through the Port. It's vital to the commerce of the State of Maryland.

So these are the things that we look at how this program can help us ensure the security of the Port. Similarly we'll be looking at it at the Airport with TSA's involvement there.

The real challenge for me as the State Coordinator for this program is how do you pull it together Statewide. We leverage what's going on in the NCR. We've also made some progress recently in the counties that surround Baltimore City and looking to bring them in. They saw the value of what this card can do.

Incident commanders will instantaneously have information from this card reader, attributes that we put on, whether it's a Hazmat profession, a medical professional. Who do I have on-site that can help me in this situation?

If we would have had this for Hurricane Katrina, we would have been able to do a lot more a lot faster. We've learned that.

So I think our job today in showing the strategic partnership that we have in the National Capital Region is

to show how this can be applicable for you in your states that don't fall within that region, but how it will help out in the long term by going to a common credential.

We have gotten support from MEMA, which is the Maryland Emergency Management (Agency) folks; our Department of Homeland Security. Our Governor is certainly aware of the initiative that we're working on here, and we look forward to making this successful.

As we look down the road, we look at the other types of credentials that are coming online, whether it be Real ID or Hazmat CDL (commercial driver's license). HSPD 12 is driving the credentialing process in a FIPS 201 direction. We're going to see, I believe, and I'm sure the folks here believe, that that's the common credential platform that's going to come down the road. We want to be out on the tip of the spear embracing that technology today so when these follow-on requirements come down the road, we'll already have that common platform and we'll make transition and make implementation of those projects a lot easier.

At this time I want to turn the program over to Jack Markey from Frederick County, Maryland.

MR. MARKEY: Thank you. It basically comes down

to trust, and I think that's one of the sometimes overused words. I spend part of my days as a uniformed Assistant Chief in the Fire Department, and I'm also the Director of Emergency Management for the County. I often experience a very different approach from people when I'm in uniform versus when I'm not, and why is that?

In a lot of cases it's because they think they know who I am when I'm in that uniform. Unfortunately, in the interesting times that we live in, sometimes that's an unsafe assumption to make.

And living where we live in the Mid-Atlantic region, particularly in Frederick County, why we're interested, we have some facilities that Lemar and the folks at the Pentagon help us protect -- Fort Dietrich, Camp David, alternate communication centers. There's a lot of folks that pass through my county that I need to know who they are because I may need to help facilitate them getting where they need to be.

So without an extensible architecture that I can trust -- not just because it says I work for the Pentagon, but I can prove that that gentleman works for the Pentagon -- for our folks who provide mutual aid fire and emergency services support on one post at Fort Dietrich, when we

arrive at the gate, do they trust that we are who we say we are? Can we prove we are who we say we are, and can we continue to do that as we work forward together?

We, like VDOT and MDOT, were engaged in our own projects for identity cards and looking at making independent investments, and what we found with the first responder partnership with Tom Lockwood's office and Craig is that we want to make those investments together in a common platform that we know will work for all of us, not just piecemeal where we still end up with sixteen different cards because we need to talk to and interact with sixteen different people.

We need to leverage that trust. Citizens trust us because we're in uniform. We recently had staff from my division of Fire and Rescue Services and from other parts of the State of Maryland respond via Operation Lifeline to the affected Gulf (of Mexico Coast) States in the aftermath of Hurricane Katrina . . .

Dr. Elmer Carreno, who's been part of this preparedness and partnership initiative, was among the team that went down there. He and…other physicians arrived and were basically denied the ability to save people's lives for 48 hours until they could determine were they really

doctors or not.

This is the exact type of circumstance that we're trying to address proactively here before those types of emergencies confront us here.

If someone were to ask me ten years ago would Frederick County Emergency Responders be in Gulf Port, Mississippi, be in New Orleans, Louisiana, I'd have looked at you like you were crazy, but that is exactly what happened, and many of the other jurisdictions within the State of Maryland, the State of Virginia, and others here responded likewise.

But when those personnel arrived there, there was little or no way to prove who they were other than the fact that they were in uniform, they were on a fire truck, so they must be a firefighter, and as we look going forward, I'm not convinced that that's where we need to be.

We're engaged in our own process. Just speaking within the Fire and Rescue, we operate 32 Fire and Rescue facilities, 29 of which are operated independently of the county government by independent fire and rescue corporations. They can go do their own thing. We're looking to bring them into this fold and say we have firefighters that could be working at any of those 29 fire

stations on any day.

We don't want the proliferation of a card vendor for each station, for each place they have to go, and we think that model, as Tony said, scales not only to the state level, but also to the national level.

I only have one identity. Why do I need multiple cards to prove I am who I am?

I guess the last thing I'll leave you with is we're really reviewing this as a gateway technology, and Tony says it well. This is a platform. This is where we can start going forward together -- data security, access control, actually knowing the attributes about someone in a way that we can verify.

This is where we need to be in the emergency response community because without it, it deprives us of all the resources that come to assist us, or we open ourselves to considerable risk.

Somebody arrives as a person falls down on the floor and says, I'm a doctor. That's one case. But when you're looking at it from an organizational perspective, from planned events like we have in the National Capital Region in the District where emergency response is wherever we go, we can't just play, The person's in a uniform.

That's good enough. Those days sadly I think have left us.

With that, I'll bring up Chris Tonjes from the District of Columbia.

MR. TONJES: Good afternoon. My name is Chris Tonjes. I work for OCTO (Office of the Chief Technology Officer of Washington, DC), and we are embarking on a citywide credential program for all 34,000 District government employees. When we began this program, we originally were going to use our own [solution] and proprietary technology.

Once we joined the NCR First Responder Partnership Initiative, we decided that it would be instrumental for us to comply with the guidelines of FIPS 201 in order to be HSPD 12 compliant.

We'll be issuing a uniform credential to all employees beginning November 15. We think that this is an extremely important program for us to follow because many of our ESFs and first responders will require access to federal facilities, and we also have coordinated the upgrade of our physical security access readers to coincide with the issuance of these cards.

Our partner agencies in this are Protective Services Police Force, the District Office of Personnel,

the District Office of Property Management, and also Fire and EMS (emergency management system).

We want all City employees to have one card that does a multitude of things, and we found that this standard we're able to apply quickly, and we're very, very pleased to be a part of it.

MR. WILSON: With that in mind, you've heard from a variety, as I said, of state, local, and regional governments who are part of the strategic partnership that we have for this initiative, and I'll now open the floor for any questions. Sir?

[In answer to an inaudible question from an audience member:]

MR. CIERI: [Restating the question,] What are the costs involved and whatnot? So we're setting up a concept within the federal government so that it's Schedule 70, so that state and local municipalities can buy off the government buy. That should be in place by . . . It should have been in place by the end of November, and most probably will be in place before the end of the calendar [2005] year.

The price, you just looked at the price of the card. The price of the card with all the technology on it

personalized would be about $8 per card, but that's not where all the costs are. The cost is in the infrastructure that feeds this. What is a huge benefit to you here is that on the Fed side, they're putting in place the ability to offer you that infrastructure at little or no cost.

So if you want to explore that further, are you in the NCR? . . . Well, if you want to explore that further, what I would like you to do is we could take that off line. You can send an E-mail to Craig. We'd get into infinite detail with you if you want to explore that.

MR. WILSON: Sir?

[In answer to an inaudible question from an audience member:]

MR. CIERI: First of all, we're dealing with, on the federal level, a national biometric standard for interoperability. It's one of those things that you can go up and punch up and get all the detail of. It's Special Publication 800-76. That is still in draft format. It's intended to be finalized by the end of the year. That would be using fingerprint technology.

The issue is right now we are also coinciding with the ISO (International Standards Organization) standards for crossing borders, which takes the digital

photo and puts that, embeds that into the chip of the card. So there is no one way that you tie the card from the issuer to the bearer except going through the entire process, which includes offering a PKI certificate along with biometrics starting with the digital picture. Did I answer your question?

AUDIENCE MEMBER: Thank you.

MR. CIERI: It's like you play the way you practice. Now, the interesting thing about all this, this has nothing to do with the card or the technology that feeds the card. It has everything to do with the preparation for what is going to happen, and running the exercise to shine the light on what are our frailties, and using the National Capital Region as the guinea pig.

Just imagine what the federal government has done. They've put a standard in place. Now, listen to this one, it's an unheard of story: They've put a standard in place, and what they've gone ahead and said was, We're going to eat our own dog food. We're going to do it to ourselves, and we're going to do it to ourselves in the next two years. Where did you ever hear that story before?

We will only get there by doing, and the doing is the exercises that lead us to, What is the trust that we

really need? What does Lemar need at the Pentagon? What does Mike need at the Pentagon when that request comes in to take over the Smart Traffic Center?

[In answer to an inaudible question from an audience member:]

UNIDENTIFIED SPEAKER: An M-16 going along with the request.

MR. WILSON: Yes, sir.

[In answer to an inaudible question from an audience member:]

MR. WILSON: I'll give it to the person who fits the bill, right? Lemar?

MR. JONES: I also represent a community some of you may know as "Blue Badges," the intel (intelligence) community where some identities need to be protected. The same identity that needs to be protected when they walk into your place of business, that card will still say the same things that their card says right now. So their identity is covered as we speak today because they put the attributes on the card at the organization that's issuing the card. So we will not compromise anyone's identity if they haven't already compromised it themselves.

MR. WILSON: Sir?

[In answer to an inaudible question from an audience member:]

MR. CIERI: Robert LeGrand is in the room, also from DC government. But look, what do we need to feed the handheld? It could be you booted up if you have com (communications) out to a network or a GPRS (wireless) link. You do need some com to run the revocation list to the handheld. The com then goes away. It's as good as the last time you did it.

Let's talk about power. Do I need power? Sure, I need power. Eventually I've got to feed this thing, alright? So there are some issues beyond the credential that we need to attend to, and that's what we intend to prove by the exercises.

What is it that we need? Do we need these mobile devices to bring us power? In these times . . . we can use satcom (satellite communications).

MR. WILSON: I'll take one more question. Yes, sir.

[In answer to an inaudible question from an audience member:]

MR. CIERI: I've been told be nice, so I'm going to try to be nice. The question you're saying to me is you

have 25,000 volunteers, well-intentioned people that want us to provide service, and we want them to provide the service. We also want to be trusted on the other side, whether they're in their community or outside their community.

So at this point in time someone in some way with some process has identified those folks, have vetted them in some way, have said you have a certain specialty, and they have that trap in some type of . . . whether it be some type of database, whatever that is, that now holds that resident within those different volunteer camps.

We're not saying to change that whatsoever. We need that to continue. What we need to do is work with you so that the right interface exists so that the credential that they receive has these attributes to it, but they have to continue to maintain what they maintain today.

I don't want you shipping that to the federal government. I want you to maintain it and secure it in a way that it can be trusted at another end, and I don't know if I answered your question.

Where is the funding coming for that? The funding for that is what funding do you use now?

[In answer to an inaudible question from an

audience member:]

MR. CIERI: Then I would respond in another way because I wanted you to get to that point. Then what we need to do is shine the light on that very issue and either go after grant money or go after the Governor to understand these very issues so that we can get them the funding that's required to do that.

This is not a talk session. This is a do session, and that's what exercises will do. They will shine the light on our frailties.

MR. WILSON: Before we close, I was asked by Brad to paint a scenario for you of where we're going with this that you can understand how you can use this in the practical application sense.

For example, right now one of the things that I've learned when I go around the region, and I've talked to the firefighters and the fire chiefs and the police officers, it baffles me that we've put so much money in technology at the top, at the strategic level and the operational level, but very little funding, as the gentleman said in the back, at the tactical level. The firefighters still show up, and they still turn in this cardboard placard with their stats on it.

So we have all these coms, all this sophistication, but they still use this placard, this cardboard placard that's vital to them, to their person for when they go into the fire.

It may have blood type on it, it may have whatever on it, but they go into the fire and they come back, and they pass all the placards back to the fire chiefs. They count and make sure they pass them out and make sure everybody's there, and then they go.

Well, with this technology you can actually, as you're loading on your fire truck, getting on your fire truck, you can transmit to your Emergency Operations Center who's on the truck, who's inbound, and what assets you have available to you.

So for example, you may have five firefighters, but each firefighter has different quals (qualifications), maybe three quals apiece. So you have fifteen qualifications. Maybe somebody speaks Farsi.

Maybe you go into the fire. When you get to the fire scene, you need somebody who speaks Farsi, but how do you know? You don't know because you've got firefighters in there. So you call back and you say, "I need somebody who speaks Farsi."

They're right there.

So you have asset management. You get to the scene. There's management there. So when you come into the scene, the commander knows who's come in, knows the human resources and the mutual asset management. Then when you check out, you check out electronically, and while you're there not only can you check in to say that somebody's inbound, here are their stats, here's their blood type. So if you need more blood, you know you can go right away.

Electronically--you can do all this electronically without ever touching paper. So when they come in, they go to the scene, they do their thing, they check out. While they check out, if it's an [inaudible] community, for example, the firefighter, the firefighter who's running the [inaudible] shop, he or she can then electronically digitally sign the report, send it back to the Emergency Operations Center, and they leave, and the Emergency Operations Center can then go back into all that's been involved and put in for reports, and electronically sign that and send it on to your Emergency Management agencies or whatever. But you have done everything electronically without ever touching paper.

So these are some of the things that you can do for your scenarios with respect to how you can use this technologies for mobile identity management, logical access, physical access, or for controls.

MR. JONES: This morning at the Pentagon we did an evacuation exercise at a federal office building to the Navy Annex. We actually evacuated 4,000 people. We used a handheld mustering system where we actually accounted for 4,000 people within the span of about 50 minutes at the assembly areas to actually be able to tell the incident commander who had gotten out of the building, who was missing in what part of the building, and where did they need to send their fire rescue into the building.

So as Craig is trying to illustrate in a scenario, we actually executed the scenario today with 4,000 actual live bodies to make sure that it would remotely transmit to a receiver so we can actually give a fireman, "Here's where you need to go, here's where we're missing people, let's go in and recover whoever we need to recover," and it's a practical application.

So the tools are there. We just now have to figure out a way to get them further into the environment, just not at DOD or not at VDOT or not at MDOT or not at

Frederick County. We're trying to make this a national kind of thing.

MR. WILSON: Thank you very much.

(end of session)