DEPARTMENT OF VETERANS AFFAIRS SMART CARD PROJECTS

HEARING

BEFORE THE

SUBCOMMITTEE OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

OCTOBER 6, 2004

Printed for the use of the Committee on Veterans' Affairs

Serial No. 108–52

U.S. GOVERNMENT PRINTING OFFICE
98–848PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON VETERANS' AFFAIRS

CHRISTOPHER H. SMITH, New Jersey, *Chairman*

MICHAEL BILIRAKIS, Florida
TERRY EVERETT, Alabama
STEVE BUYER, Indiana
JACK QUINN, New York
CLIFF STEARNS, Florida
JERRY MORAN, Kansas
RICHARD H. BAKER, Louisiana
ROB SIMMONS, Connecticut
HENRY E. BROWN, JR., South Carolina
JEFF MILLER, Florida
JOHN BOOZMAN, Arkansas
JEB BRADLEY, New Hampshire
BOB BEAUPREZ, Colorado
GINNY BROWN-WAITE, Florida
RICK RENZI, Arizona
TIM MURPHY, Pennsylvania

LANE EVANS, Illinois
BOB FILNER, California
LUIS V. GUTIERREZ, Illinois
CORRINE BROWN, Florida
VIC SNYDER, Arkansas
CIRO D. RODRIGUEZ, Texas
MICHAEL H. MICHAUD, Maine
DARLENE HOOLEY, Oregon
TED STRICKLAND, Ohio
SHELLEY BERKLEY, Nevada
TOM UDALL, New Mexico
SUSAN A. DAVIS, California
TIM RYAN, Ohio
STEPHANIE HERSETH, South Dakota

PATRICK E. RYAN, *Chief Counsel and Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

STEPHEN E. BUYER, Indiana, *Chairman*

MICHAEL BILIRAKIS, Florida
TERRY EVERETT, Alabama
JOHN BOOZMAN, Arkansas

DARLENE HOOLEY, Oregon
LANE EVANS, Illinois
BOB FILNER, California
TOM UDALL, New Mexico

CONTENTS

October 6, 2004

DEPARTMENT OF VETERANS AFFAIRS SMART CARD PROJECTS

WEDNESDAY, OCTOBER 6, 2004

U.S. House of Representatives,
Subcommittee on Oversight and Investigations,
Committee on Veterans' Affairs,
Washington, DC

The subcommittee met, pursuant to notice, at 9:35 a.m., in room 334, Cannon House Office Building, Hon. Steve Buyer (chairman of the subcommittee) presiding.

Present: Representatives Buyer, Boozman, and Hooley.

OPENING STATEMENT OF CHAIRMAN BUYER

Mr. Buyer. The Subcommittee on Oversight and Investigations of the Committee on Veterans' Affairs will come to order. This is a hearing on the issue of the VA's smart card projects. The date is October 6, 2004, and good morning.

The importance of today's hearing on the implementation of VA's smart card projects became very evident to us last August when the FBI issued a warning in a bulletin, in a weekly bulletin to law enforcement. The bulletin suggested "al Qaeda terrorists looking for a U.S. military target might try to attack a VA hospital rather than a base or other high security installation." The bulletin went on to say, "These facilities may be considered attractive targets due to their association with the military and a perception that such an attack may be more successful than an attack against traditional military targets which generally maintain a more robust security posture."

In these uncertain times, the VA needs to know that people coming in and out of their facilities are in fact who they say they are. Today's hearing will examine the advantages of using smart cards, which include identity of individuals accessing VA buildings and computer systems, cyber security, employee accountability, and fraud prevention in the compensation and pension delivery systems.

In addition to standard features such as bar codes or magnetic strips and digital photos, today's smart cards have the capability of storing biometric data such as fingerprints or iris scans.

It seems that even today's smart card technology, which has been loaded with biometric data, may not be sufficient to prevent all breaches of security. In order to ensure data integrity and authenticity in VA's benefits deliver that is being conducted electronically, the VA will have to introduce "public key infrastructures," which are commonly known as PKIs. PKIs? P-K-Is. Not commonly known to this guy. (Laughter.)

PKIs are systems that provide for verification and authenticity of VA employees involved in an electronic transaction. PKIs can ensure that parties to an electronic transaction are really who they claim to be and the information has not been altered or shared with any unauthorized entity. This involves a system of computers, software and data that relies on certain cryptographic techniques such as digital signatures.

Even though smart card technology has been available since the mid-1970s, its widespread use by the federal government is something that is now being seriously undertaken by many government agencies, including the Department of Veterans Affairs. In fact, it was mandated in Homeland Security Presidential Directive 12. It was titled the Policy for a Common Identification Standard for Federal Employees and Contractors, that a government-wide standard for secure and reliable forms of identification be established and it shall be implemented by each agency within six months.

Since the VA announced its plans to implement a veteran-specific information smart card during an oversight hearing back in September of 2000, there's been really very little activity by the Department in the development and implementation of other smart cards. The VA beneficiary smart card has yet to be implemented and is something that needs to be accomplished. The Subcommittee will look at this in more depth at a future hearing.

In preparing for today's hearing, I was pleased to learn that the VA is working with the Department of Defense, the General Services Administration and the National Institute of Standards and Technology in the development of its Authentication and Authorization Infrastructure Project, which is being designed to provide the capability to authenticate users and systems within the Department. The VA is using the GSA's standards-based contracting vehicle, which was also used by DOD in the development of its common access card. It's good to know that the VA isn't trying to move in another direction and is adhering to GSA's contracting model.

I'd also like to take the opportunity to thank Secretary Principi for his strong leadership and commitment in moving the VA forward with its implementation of the presidential mandate on smart cards. I'd also like to congratulate the Secretary and the members of his IT team for keeping a disciplined approach in its planning and implementation of this very important project. That's the good news.

There are a number of good reasons why the VA needs to adopt this technology. Any VA smart card project will reduce costs, help prevent fraud and abuse in the benefits system, while also ensuring greater confidentiality of private information.

With the growth and implementation of identity systems comes an increased need to ensure that authentication technology is of the highest possible standard. Security is an issue that affects all citizens, and it would be a disservice to the American veterans to forge ahead with smart card technology without undertaking the necessary investigations and precautions. It is the job of the Oversight and Investigations Subcommittee to highlight the best practices that define the development of smart card technology and encourage its progress and Department-wide implementation.

With that, I will now yield to the Ranking Member for any comments she may have by way of an opening statement.

OPENING STATEMENT OF HON. DARLENE HOOLEY

Ms. HOOLEY. Thank you, Mr. Chair. I, too, would like to thank the witnesses for testifying today, and I would also like to thank you for holding this hearing, Mr. Chair.

By all accounts, including the written testimony for this hearing, VA is on the right track with the implementation of the smart card program. Full implementation of VA's Authentication and Authorization Infrastructure Project will favorably impact a wide array of programs important to VA. It will be a cornerstone of physical security and control access to VA's comprehensive storehouse of sensitive personal information. It will help align strategies to comply with the Health Insurance Portability and Accountability Act and a host of other important regulatory compliance requirements.

VA has accelerated its implementation plan for this project to the point where it now must wait for additional guidance from the National Institute of Standards and Technology before proceeding further with such initiatives as adding biometric requirements to the card. Not only is the card smart; at this point in time, its managers appear smart as well.

Fielding the smart card is a great goal. It is not a universal panacea or cure-all for all programs. As Mr. Brandewie notes in his statement, a prelude to issuing the card is a requirement for strong authority of the individual. The card may be a tough cookie to crack, but it is essential to assure the identity of that person before the card is issued as verification of that person. He notes that this is the age of identify theft, and a process that does not guard the possibility of wrongful issue will be faulty, especially when the biometric component is added to the card.

Mr. Chair, I am very optimistic about the potential promise of this card, and I yield back the balance of my time.

Mr. BUYER. Thank you. We'd like to now move to the first panel. It is the Honorable Benjamin H. Wu, the Deputy Under Secretary for Technology, Technology Administration, Department of Commerce. And we also have Ms. Linda Koontz, the Director, Information Management Issues, United States Government Accounting Office.

The Honorable Mr. Wu, you may begin.

STATEMENTS OF BENJAMIN H. WU, DEPUTY UNDER SECRETARY FOR TECHNOLOGY, TECHNOLOGY ADMINISTRATION, DEPARTMENT OF COMMERCE; LINDA D. KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY VALERIE C. MELVIN, ASSISTANT DIRECTOR, INFORMATION MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF BENJAMIN H. WU

Mr. WU. Thank you, Chairman Buyer and Ranking Member Hooley. I want to thank you for this opportunity to testify today about our Department of Commerce's smart card activities at NIST, our nation's oldest federal laboratory and the crown jewel of our federal laboratory system. I want to commend you for your leadership to implement smart card technology at the Department of Veterans Affairs, and I appreciate your confidence in the attack of the NIST technical experts to effectively commercialize smart card technologies.

NIST plays an important role in cooperation with other federal agencies to eliminate the roadblocks to widespread deployment of smart cards. NIST works with industry and other government agencies to provide interoperability specifications, standards and guidelines, with a goal of expediting open and interoperable methods for smart cards.

NIST will be leading also the President's assignment to the Department of Commerce's requirements under the Homeland Security Presidential Directive HSPD–12. NIST has also done considerable work in the area of biometrics under the auspices of the USA Patriot Act.

Mr. Chairman, I know that your interest in utilizing smart cards at VA facilities stems from its ability to improve the security of critical infrastructure both from a physical and a logical perspective. Since smart cards are capable of performing cryptographic functions, they can perform important security services such as securely storing digital signatures, holding public key credentials and authenticating a claimed identity based on biometric data. As such, smart cards are a crucial element in a range of current and expected critical applications and programs. They are also the underlying foundation for the standard recently required by HSPD–12.

NIST's smart card program dates back to 1988 when NIST chose to invest in significant early stage research upon recognizing the potential of smart card to improve the security of federal IT systems and also our national information infrastructure. The NIST smart card program produced many early innovations in the areas such as generic authentication interface for smart cards, the first cards to implement the Data Encryption Algorithm, the Digital Signature Algorithm, and the first reprogrammable smart card. And these innovations are really the foundation of today's cutting edge smart cards that are being used in the private sector as well as the public sector.

In the government, while many federal agencies have a longstanding interest in smart card technology, large scale deployment of smart cards has proven challenging. The agencies have found it difficult to deploy large scale smart card systems due to a lack of interoperability among different types of smart cards. And without assurances of interoperability, agencies would be locked into a single vendor. Stressing this issue of interoperability is critical before significant investments can be made.

Additionally, smart card systems have historically been driven by requirements arising from specific application domains such as banking, telecommunications and health care. And this has led to the development of smart cards that are customized to the specific application requirements of each domain, with little interoperability between the domains.

And these vertically structured smart card systems are expensive, they're difficult to maintain, and they're also based on proprietary technology. So GSA created a contract vehicle and a program to procure interoperable smart card systems and services, and to promote and facilitate the use of this critical security technology within the federal sector. And after much work to address the federal customer needs that are identified, NIST published two versions of the Government Smart-Card Interoperability Specification, also commonly known as the GSC–IS. They did that in June of 2002 and 2003, respectively.

The GSC–IS has been well received and is making a significant impact. Accordingly, many federal agencies are moving forward with plans to deploy large numbers of GSC-compliant systems, including DOD's Manpower Data Center and their CAC Operation Office.

In addition to our work on the GSC–IS, NIST is also focusing on standardization and conformance testing. GSA and other federal agencies have long sought to avoid the problem of being locked into that proprietary, non-interoperable smart card technology. Recognizing the need of an increased federal customer base, NIST is working with ANSI, which is the American National Standards Institute, our national standards body, and the International Organization of Standards, ISO, to standardize the specification. And in January of 2003, GAO issued a report in January that listed the progress for the federal government adopting smart card technology. The report urged NIST to continue improving and updating the government's smart card interoperability specification by addressing government-wide standards for additional technologies, such as contact lists, biometrics, and optical stripe media, as well as integration PKI to ensure the broad interoperability among federal agency systems.

In response to these GAO recommendations and identified federal agency needs, NIST is examining requirements for and issues associated with definitions of a multi-technology card platform. NIST is also engaged in holding a number of workshops to make sure that we are able to move forward on this multi-technology card. These workshops have been very successful. The last one last one was completed in March of 2004, and based on the proceedings in the workshop and also with subsequent interviews conducted with the user community, NIST produced a technical report that has identified integration and interoperability research topics, gaps in standards coverage and also multi-technology composition issues.

And then earlier in July of 2003, NIST published the most recent version of GSC–IS, Version 2.1. And that document addresses the remaining GAO recommendations by providing support for biometrics, contact lists, smart card technology and also PKI.

We're also looking at the conformance testing for smart cards, which is another critical element of the utilization and the broad dissemination of smart cards technology. But the most important thing that we're working on right now is the Homeland Security Presidential Directive 12. HSPD–12 was issued on August 27, 2004 by the President, and the directive calls for the Secretary of Commerce to issue a federal standard for a secure and reliable form of identification issued by the federal government to its employees and contractors, including contractor employees.

The NIST standard will include graduated criteria from least secure to most secure to ensure flexibility and then selecting the appropriate level of security for each application. It's quite obviously an ambitious assignment, one that will considerable aid the federal homeland security efforts. And while developing the standard required by HSPD–12, we will ensure that ample privacy protections are also included.

NIST has taken the lead in development the standard and has developed an aggressive timetable to meet the six-month deadline. NIST is working with OMB and other departments and agencies to take advantage of the efforts currently underway within the federal government, and NIST is also working with public and private sectors to develop the standard.

Today NIST is holding a workshop with over 80 federal agency representatives to discuss the development of this very standard. And additionally, tomorrow, on the 7th of October, NIST is holding a public workshop for industry and others to discuss its plans and to solicit feedback from the private sector.

By developing a viable commercial marketplace for smart card technology in the United States, we can increase the competitiveness for the U.S. smart card industry in the global market while also protecting and improving the security of our nation's critical infrastructure. NIST is going to continue to improve and update smart card interoperability specifications and actively participate in federal coordinating efforts. We look forward to working with the Veterans' Affairs Administration as well, and also this committee.

So I will thank you for the opportunity to testify on behalf of NIST, and I'd be open to any questions you may have.

[The prepared statement of Mr. Wu appears on p. 35.]

Mr. BUYER. Thank you very much. Ms. Koontz.

STATEMENT OF LINDA D. KOONTZ

Ms. KOONTZ. Thank you, Mr. Chairman, Ranking Member Hooley. I appreciate this opportunity to participate in this hearing regarding the adoption and use of smart card technology. Valerie Melvin is with me today. She is the Assistant Director responsible for our work at Veterans' Affairs.

At your request, my remarks today will summarize the federal government's efforts toward adopting smart card technology, along with the challenges that have been encountered. Also included is an overview of the actions that the Department of Veterans Affairs is taking to implement smart cards.

The unique properties and capabilities of smart cards offer the potential to significantly improve the security of facilities and buildings, systems, data, and transactions. With the potential uses and associated benefits in mind, the Office of Management and Budget, the National Institute of Standards and Technology, and GSA have taken actions to advance the adoption of smart card technology government-wide.

Among GSA's contributions toward promoting this technology was its efforts in 2000 to develop a standard contracting vehicle for use by federal agencies in procuring commercial smart card products from vendors.

Further, OMB issued a framework of policy guidance for government smart card adoption in July 2003 in a memorandum detailing actions the administration was taking to streamline authentication and identity management in the federal government. The National Institute of Standards and Technology for its part has continued to improve and refine its smart card interoperability standard.

In turn, federal agencies have launched numerous projects offering many capabilities and tangible and intangible benefits. As of June 2004, 15 federal agencies had reported 34 ongoing smart card projects. Further, as understanding of smart card technology has increased, agencies have begun pursuing larger integrated agency-wide smart card systems aimed at better securing both physical access to facilities and logical access to computer systems and networks.

Nonetheless, agency managers have faced considerable management and technical challenges in their efforts, including sustaining executive-level commitment, recognizing resource requirements, integrating physical and logical security practices, achieving interoperability, and maintaining system security and privacy of personal information.

These challenges have become less formidable, however, as management concerns about securing federal facilities and information systems have increased, and as technical advances have improved the capabilities and reduced the costs of smart card systems. The challenges are also tempered as increased federal guidance brings direction to agencies handling other smart card initiatives.

The Department of Veterans Affairs is among numerous federal agencies currently pursuing large scale, agency-wide smart card initiatives. VA's Authentication and Authorization Infrastructure Project, begun in 2002 and currently in limited deployment, is planning to employ a combination of smart card and other technologies to achieve the capability to authenticate users with certainty and grant them access to information systems necessary to perform business functions.

As a result of this project, VA anticipates between 2005 and 2009 issuing 500,000 smart cards to its personnel at an estimated cost of about $162 million. While this project is still under development, VA has gained experience through its own prior efforts, and as a participant in government-wide initiatives to further smart card adoption. These experiences should better position VA to be successful in its efforts to implement smart cards as an essential means of securing critical information and assets.

That concludes my statement. I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Koontz appears on p. 41.]

Mr. BUYER. Mr. Wu, I enjoyed your written statement. As a matter of fact, I had to read it twice. It's just me. I had to read it twice, and what struck me the most was this drive that has been in place for quite a while for all government agencies to have what you described as this interoperability on standards and guidelines.

So we've got this goal. At the same time, we have many different agencies, and you're right, that have their own specific requirements. At the same time, you have a lot of vendors out there with their own ideas on how to provide things and their proprietary interests. And so you really sort of have some competing interests. And I'm trying to figure out really who's in charge of the oversight. Who would be in charge of the oversight on all these government agencies to make sure that we don't have all these stovepipes? Who—I don't even know—who is in charge?

Mr. WU. Well, I think the GSA is in charge of the federal enterprise.

Mr. BUYER. Okay.

Mr. WU. And this provides the technical expertise that allows us to congregate on a particular standard that allows for interoperability or to allow for a suite of standards in which we can have a platform in which then other people can build upon that would be open, that would be industry-led, that would be market-driven.

And so while NIST plays a critical role in trying to drive interoperability, GSA would have the programmatic functions. I testified on this subject last year before Congressman Putnam's subcommittee within the Government Reform Committee, and Congressman Putnam was advocating much the same that this Subcommittee is doing, to try to make sure that smart card technologies are being deployed and utilized effectively throughout the federal government.

He identified at that time that GSA should be the lead. NIST does provide a critical technical role that will help facilitate the process, and we work very closely with GSA as with all the other federal agencies in an interagency way.

Mr. BUYER. All right.

Mr. WU. The President's directive, HSPD–12, further underscores the need for us to work collaboratively, especially as we move toward this critical need and try to address the homeland security applications. And once again, NIST there will be driving on the technical aspects, with the intention of trying to create and promulgate a standard that will be effective.

Mr. BUYER. All right. Just because Chairman Putnam thinks that they're in charge, does GSA know that they're in charge, and do they have the authority to be in charge?

Mr. WU. My understanding is yes. Certainly they understand their role and their functions, and they're taking it seriously.

Mr. BUYER. Taking it seriously. In your own testimony, though, you say that large-scale deployments of these smart cards is difficult due to the lack of interoperability among different types of smart cards.

Mr. WU. Well, that's for the current smart cards or the current systems that are in place. We do have smart cards being used in various federal agencies or for various functions, and they have, unfortunately, for the most part a lack of interoperability.

Mr. BUYER. All right. Break. Give it to Bubba here, all right? If I'm a doctor and I am, let's say, a doctor who's a reservist and I work at DOD and I have to go over to the VA, can I use my smart card and can I get equal access whether I'm at the Pentagon, whether I have to go to, I don't care, Fort Lee? And then I come back and I want to stop in at the VA. Can I utilize that smart card for that access?

Mr. WU. I think that is the hope. Right now, that's not the reality, but I think DOD has taken on a model program within their CAC program to try to utilize that card that can be used throughout all the DOD functions and to then——

Mr. BUYER. Okay. Can I—time out for a second. Because what is driving me insane is DOD will buy something, I don't care whether it's a medical piece of equipment to whatever, they buy what they want to buy for their own reasons. The VA buys what they want to buy for their own reasons. And I love your statement, because we're talking about how we want to make everything interoperable and we want to do the deployment, but we recognize there are problems because of specific requirements within specific domains, but how do I do this? How do I say to the VA, stop; I don't want you to deploy anything out there until it's interoperable, and you've got to show me that it's interoperable with DOD. And DOD, I know you're out in front there, but we want to make sure that we've got interoperability here. Because if we can't do it between VA and DOD, what makes us think that Treasury is going to be able to do it with Justice, where they should also be just as equally interoperable? So let me just throw that to you.

Mr. WU. Well, that is a big challenge, and that's why the importance of standards can't be said enough. We need to have standards that allow for that interoperability. HSPD–12 recognizes the need for us to coalesce around a standard. The hope is that we can use the efforts for HSPD–12 as a lever to further work on our standardization for interoperability.

NIST, through ANSI, through ISO, through their standards development organizations, through our interagency working group, through the GSC–IS, has already been working towards that goal. HSPD–12 puts an exclamation point on it and says that not only do we need to move towards a standard, we need to do it very quickly because of national security and homeland security and homeland defense concerns.

And so the hope is that that effort, HSPD–12, will serve as a lever to expedite this process.

Mr. BUYER. Ms. Koontz, do you have any comments on what we've just discussed?

Ms. KOONTZ. I would just add to your earlier question about who's in charge. I would want to point out that the Office of Management and Budget, from a policy perspective, is in charge of smart cards. And they have issued, as of last year, a policy which begins to drive the federal government toward interoperability.

We also commented in our previous report about the role of GSA, which is to promote and facilitate smart card implementation, but we thought there was more that GSA could do in terms of having a strategy for government-wide implementation.

Mr. WU. Mr. Chairman, I should also add that I agree with Ms. Koontz's point about OMB. And OMB has taken on this issue at the highest levels. Clay Johnson, who is the deputy director of OMB, has personally overseen a lot of the actions for HSPD–11, which I've been most engaged on. And he's also keeping a very close eye to make sure that the President's directives are also met in a timely manner.

Mr. BUYER. You know, I'm going to yield to you, but, you know, here's part of my challenge that I think as a committee we face. You know, we've been spending billions of dollars over the last decade in developing these stovepipe electronic medical records. And then, you know, DOD and VA can't share certain things. I'm just throwing this out here. I love this interoperability, but the reality is—boy, if we can achieve this, this will be very exciting.

Ms. Hooley?

Ms. HOOLEY. Thank you, Mr. Chair. Ms. Koontz, thank you for your excellent and informative report on smart cards. The technology behind the cards seems strong, with the inclusion of a biometric component very strong. Once created, my understanding is the system will accept the smart card as a strong indication that the person has the access that the card indicates. How deeply did GAO look into the front end of the security system? How strong are the processes for assuring the identity of the individual before the issuance of the card?

Ms. KOONTZ. That was something that I believe was not within the scope of our previous work. But that could be an issue of further study, I think.

Ms. HOOLEY. Okay. Mr. Wu, how coordinated is this process among the agencies?

Mr. WU. Within HSPD–12?

Ms. HOOLEY. Uh-huh.

Mr. WU. Very much so. We have today ongoing a meeting with all the federal agencies, and then tomorrow we'll be continuing the discussion with affected stakeholders from the private sector. And so we're trying to make sure that we have input from both the public and the private sectors. Because ultimately, when you're trying to achieve commercialization for these smart card technologies, you need to rely on the private sector as well.

And so, making sure that we've got private sector input is very important, and so we're not doing it just for the public sector, but also within the private sector as well.

Ms. HOOLEY. How does a vendor get involved in the process? I mean, are you looking, as you're looking at cards that are interoperable, how does that vendor or vendors or the private sector fit into this whole program?

Mr. WU. Well, let me turn it over to Jim Dray, who has been engaged with the HSPD–12 efforts, and he is our technical expert from NIST, and he can explain the process in which we've developed for soliciting both public sector and private sector comment.

Ms. HOOLEY. Okay. Mr. Dray?

Mr. DRAY. Thank you. Through the history of the technology smart card interoperability program, we have worked with both the private and public sectors. There is an organization that we established early on called the Government Smart Card Interagency Advisory Board, or IAB, that was chaired by GSA for a number of years and now is chaired by Bob Donaldson of Interior.

But in any case, that committee has both public and private sector members on it. All of the contractors who are selling products through the GSA contract vehicle are members of that organization.

We also have a public comment period, as you probably are aware, for FIPS. And so we will be putting out a document we hope in the early November timeframe, a draft of the FIPS standard in response to the HSPD–12 requirement, and that will go through a public, a completely open public review period. At the end of that time, we will compile all of the public comments and respond to those and modify the document as necessary.

Ms. HOOLEY. What I'm trying to get at is if you have—if you're looking to private companies, are you going to pick one? Are they going to combine their technologies? Is it going to be the company with the best technology combined with what the public sector is doing? Just tell me how that works.

Mr. DRAY. Okay. It's actually fairly straightforward. We certainly don't want to lock this into one or two vendors. We want it to be a multi-source standard and system. And our method for doing that is to pursue these standards that we're working on. We already have GSC–IS 2.1. We're working with ISO an ANSI, as Ben has told you. And once those standards, our formal standards are in place, and actually including this FIPS in response to HSPD–12, any vendor should be able to implement those standards since they're openly available.

The specific details of the contractual arrangement of course are GSA's domain, and they do have a contract vehicle in place with selected vendors. But in the broader sense, we want to make sure that these are open standards that we're developing and that any vendor can implement them.

Ms. HOOLEY. Okay. Mr. Wu, how easy would it be to somebody intent on beating the system to—and if they have the machine that codes the card to take it apart and put it back together again? In other words, to break into the system. How easy is it?

Mr. WU. Well, it depends on what standards are adopted. If you have a PKI system in place or a biometric, it's very hard. And the intention is to develop a standard that will withstand any sort of manipulation or any sort of deception.

And we wanted to make sure that, in response to HSPD–12, that we create a standard that can authenticate and verify federal government employees basically to make sure that whoever uses that equipment or whoever has access to that particular area is the right person and is somebody who is supposed to be either there or have access to it.

Ms. HOOLEY. Okay. Thank you.

Mr. BUYER. I had asked a question earlier on staff, so I'm going to ask you, Secretary Wu. You were using the term and throwing it around, but what's the definition of "interoperable?" What's that mean?

Mr. WU. Insofar as HSPD–12? An official definition? I think that as we move through the process, I don't want to prejudge what the definition should be, because this is an interagency definition and one that should be acceptable. But I think generally, interoperability means that we have a system that can talk to each other, that can interrelate to each other, that we have something that's not proprietary, that we have standards that can be built upon each other that a number of different vendors can either build their products or other platforms onto to make sure that when we have procurement we have multiple vendor opportunities for competitiveness, but also to make sure that as these legacy systems are modernized or are developed in the future, that they continue to be able to be utilized and to talk to each other.

Mr. BUYER. Ms. Koontz, when the VA comes on line, are we going to be able to do this with biometrics, do you know? Or do I have to ask Mr. McFarland? Will convergence of biometric be there in time for that implementation, or should I ask that question later? I'll wait. I'll reserve that question.

I'm not picking on you, Secretary McFarland, but Ms. Koontz, the VA does not have the best track record here with the implementation of IT projects. Given your years of work in this area, what is your level of confidence that the VA is on the right track at this time?

Ms. KOONTZ. I would say based on what we've seen so far, and I'll put the caveat out there that VA is in the very early stages of this project, I'd say we were feeling that VA should be well positioned to make the smart card implementation a success.

They are moving what appears to be very consistently with the trends that we're seeing government-wide. They've had an opportunity to learn from a couple of pilots that they've already completed. They've also participated very heavily in a number of the government-wide initiatives on smart cards, and so they've learned from that as well. And finally, because of their timing, they should have the flexibility to be able to alter what they're doing to meet whatever the requirements turn out to be from the homeland security directive, you know, as that specification is being developed.

So I think we're cautiously optimistic.

Mr. BUYER. In your written testimony here, you mentioned how the VA has several hundred different types of identification cards. Do other government agencies, are they like that too?

Ms. KOONTZ. I don't have any basis to compare, and that is VA's number that they told us that they actually have several hundred. I wouldn't be surprised in larger agencies, however, if you had the same kind of situation.

Mr. BUYER. Does that practice make you nervous?

Ms. KOONTZ. It is not the best practice, no.

Mr. BUYER. Well, I agree. Do you have anything else?

Ms. HOOLEY. I don't, Mr. Chair.

Mr. BUYER. Thank you very much for your report. And Secretary Wu, thank you very much for your testimony and your work.

Again, I enjoyed your statement, whoever wrote this and helped you out and your input and substance in this statement. You really highlight the challenges that we have. Really.

I mean, I think we all want to get there, and, you know, what we've sort of accepted out here today, is that there's also out there in the private sector, there's a lot of competition going on out there. And they all want to gain access and they want their technology to be the one that's going to be used. But at the same time, we've got to figure out how we can control and make it standards based and implement it government wide. And the most important aspect is from the homeland security standpoint. And there's also from this Subcommittee's interest, I think a lot of these major fraud cases weren't found because of audits. And, you know, when I look at this $162 million of taxpayer money to implement this, when you do a simple cost benefit analysis, first you go, whoa, that's a lot of money. And then you look on the other side of this. Yes, but how much smarter can we do our business and do it effectively and efficiently, I think it becomes rather clear.

Mr. WU. Well, Mr. Chairman, there are technical hurdles and then there are programmatic and management hurdles. NIST is taking care of the technical hurdles to try to achieve consensus on an industry-led, market-driven standard for interoperability. The programmatic and management hurdles are being taken care of now we hope under the auspices of HSPD–12, and that's a powerful driver to bring all of the federal agencies together on a critical national priority, homeland security.

And so we hope to be able to leverage HSPD–12 to develop these management and programmatic challenges. And OMB, the highest levels of OMB, are really taking this very seriously. And so we thank you for your leadership in trying to drive VA towards this goal and we hope to apply this throughout the federal government.

Mr. BUYER. That's great. That's wonderful. Thank you, Secretary Wu.

Mr. WU. Thank you.

Mr. BUYER. This panel is now dismissed. Thank you very much.

We now recognize the second panel, Mr. Neville Pattinson, Director of Business Development, Technology and Government Affairs, Axalto. We'd also recognize Secretary Robert McFarland, the Assistant Secretary for Information and Technology, Department of Veterans Affairs. We'd also like to recognize Mr. Robert J. Brandewie, Director, Defense Manpower Data Center, Office of the Secretary of Defense for Personnel and Readiness, Department of Defense.

All right. Mr. Pattinson, you're now recognized for an opening statement.

STATEMENTS OF NEVILLE PATTINSON, DIRECTOR OF BUSINESS DEVELOPMENT, TECHNOLOGY AND GOVERNMENT AFFAIRS, AXALTO, INC.; ROBERT N. McFARLAND, ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS; AND ROBERT J. BRANDEWIE, DIRECTOR, DEFENSE MANPOWER DATA CENTER, OFFICE OF THE SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS, DEPARTMENT OF DEFENSE

STATEMENT OF NEVILLE PATTINSON

Mr. PATTINSON. Good morning, Mr. Chairman, Congresswoman Hooley, and members of the Subcommittee. Thank you for the opportunity and privilege to testify at this hearing on smart card initiatives at the Department of Veterans Affairs.

I am the Director of Business Development, Technology and Government Affairs at Axalto. Axalto, which is based in Austin, Texas, is the largest supplier of microprocessor smart cards. I have personally been involved with identity systems utilizing smart cards for over 7 years, including leading the efforts within Axalto for the development of the common access card for the Department of Defense. Axalto has now supplied over 5.5 million cards to the Department of Defense, along with several other government agencies.

In addition to my position at Axalto, I am board member of the International Biometric Industry Associate. I am also honored to be representing a loose coalition of three leading smart card manufacturers called the American Smart ID Card Alliance, which is a strong voice for security, privacy and efficiency of this technology and identity management.

Within Axalto, we deployed an identity management system throughout our own company utilizing smart ID cards. In order to secure our information, networks and facilities, we learned that implementing a corporate-wide identity system had several benefits. Our company realized that the information we managed, both ours and our customers', was a valuable asset that required tight security and access control. By implementing an enterprise-wide identity management system, all employees' identities were managed centrally for physical access to facilities and logical access to computer networks.

We have seen a much higher degree of accuracy and accountability as we used digital signatures and encryption on our e-mail to verify our content and maintain integrity of our information. We have also seen significant cost savings from support services.

On August 27th of this year, President Bush signed the Presidential Directive HSPD–12. This directive establishes a policy for a common standard that will allow for a secure and reliable form of identification for all federal employees and contractors that can be authenticated electronically. The Veterans Administration is ahead of many other government agencies in implementing an identity management system that credentials their employees.

We commend the Department of Veterans Affairs for embarking on its own identity management system using smart ID cards for its employees. As there are already physical access systems in place in several VA facilities, the project has embraced both a two and a three chip smart ID card. Both smart ID card variants are to contain a contact smart card chip for logical access and credential storage, along with a second chip for new physical access systems as recommended by the IAB. One of the card variants will also contain a third chip for supporting the installed base of physical access systems based on RFID technology.

The smart card project team within Veterans' Affairs has spent considerable time performing feasibility studies and prototype evaluations in many areas to ensure the correct application of the technology to their systems and processes. This planning effort will lead to a better implementation of the project as it begins its rollout to the intended VA staff and contractor population. What they have learned will also benefit other agencies in their programs as all federal agencies embrace the HSPD–12 credentialing initiative.

It is important to define the scope of an identity management system, along with specifying system-wide standards, specifications, privacy and security policies to ensure interoperability consistency and proper usage. One should use standards and open specifications, avoiding blind alleys or non-interoperability. It is important to define the criteria for enrollment and the user authentication mechanisms once enrolled. The common use of data cross agencies is also important to ensure interoperability.

The usage of PINs along with smart ID cards is a good user authentication mechanism to determine user presence with the card. However, as biometrics are becoming more commonplace and the application determines the need to increase the authentication of the user, biometric authentication should be introduced where appropriate and cost effective as either a replacement to the PIN or a security enhancing feature.

Smart ID cards are a vital link in the chain of trust of any identity management system. The ability to master identity management within an enterprise or a government agency brings tremendous savings, electronic communications security, user accountability, increased privacy and consolidated access control. Smart ID cards are a convenient, proven, portable, cost effective, highly secure technology for assisting with the management of identity. When combined with biometric,s the smart ID card offers a three-factor authentication of the cardholder: Something they have, i.e., the card; something they know, the PIN; and something they are, the biometric.

There is a wealth of experience within U.S. government agencies in deploying smart ID card-based identity management systems. The Inter-Agency Board and the Federal Identity Credentialing Committee have also endorsed smart ID cards. We need to continue to support the important effort of NIST as they advance the government smart card interoperability specification. Along with the recent Homeland Security Presidential Directive 12 declaring an aggressive timeline for all federal agencies to implement a common identification standard makes it clear that interoperability is paramount for any government agency identity system.

Thank you for the opportunity to testify before this distinguished Subcommittee. I look forward to working with the members of the Subcommittee in providing any help and guidance on this issue, and would be happy to answer any questions the committee may have.

[The prepared statement of Mr. Pattinson appears on p. 61.]

Mr. BUYER. Thank you very much for your testimony and contribution.

Secretary McFarland, you're now recognized.

STATEMENT OF ROBERT N. McFARLAND

Mr. MCFARLAND. Thank you, Mr. Chairman and Ranking Member Hooley. I'm very pleased to appear before this committee representing the Secretary and the Department's information technology programs. On March 17, 2004, I appeared before this committee and presented an overview of the VA's information technology processes and projects.

I am here today to provide an update regarding the VA's Authentication and Authorization Infrastructure Project, or AAIP. As a result of AAIP, the Department is positioned almost 12 months ahead of the mandates contained in Homeland Security Presidential Directive 12, which establishes a new policy for common identification standards for federal employees and contractors. VA has achieved this position, which is well ahead of practically every other agency, because we have continuously synchronized AAIP with government deliberations and involvement in the process that leads up to HSPD–12. We view this as a success story.

Currently, VA has a Federal Manager's Financial Integrity Act material weakness related to account management. AAIP plays a significant part in addressing this issue by creating better account management controls, two-factor identification and smart cards, and a reduction on the reliance of static passwords. The VA's Office of Inspector General has reviewed AAIP and believes it is a significant move towards removing this outstanding concern.

AIIP specifically considers and sets up strategies to effectively comply with the Health Insurance Portability and Accountability Act of 1996 Security Rule, the Gramm-Leach-Bliley Act for financial services, the E-Sign Act, the Government Paperwork Reduction Act, the Government Paperwork Elimination Act, the E-Government Act of 2002, the Federal Information Security Management Act, and OMB Memo 04–04, E-Authentification Guidance for Federal Agencies, as well as the OMB memo entitled Streamlining Authentication and Identity Management within the Federal Government.

The benefits of AAIP were apparent in preliminary tests with the Drug Enforcement Agency wherein AAIP demonstrated the ability to save up to 45 minutes in processing time associated with pharmacy transactions. This can be achieved through the application of digital signature, which complies with DEA regulations, reduces paperwork and substantially reduces unintended errors. In the process, service to the veteran is greatly enhanced in a cost-effective manner.

During detailed testing of smart card usage in "thin client" environments, AAIP demonstrated the ability to recover up to 45 minutes per day of clinician time through simplified log-on processes. VHA has tens of thousands of clinicians on duty at any given period of a day, and any recovery of productivity of this magnitude will create significant efficiencies and some cost savings, and result in better patient care for our veterans.

VA currently has several hundred thousand users of computer systems, many with their own separate accounts and passwords. This creates a tremendous account and password burden on VA to operate systems day to day. Through AAIP's use of smart cards, VA will be able to implement single sign-on technologies which minimize the number of passwords users have to remember.

VA assumed leadership over the Shared Service Provider Subcommittee of the Federal Identity Credential Committee, acting as chair. Starting in September 2003, through the collaborative efforts of the National Institute of Standards and Technology and other agencies, the SSP Subcommittee established the evaluation criteria to successfully publish a listing of qualified managed Public Key Infrastructure service providers that are available to all federal agencies. As a result, the federal government now has a core list of authorized PKI managed service providers, directly supporting an initiative identified by OMB in January of 2003.

Using this new vehicle, in September 2004, VA became one of the first federal agencies to issue a contract to a federally approved managed PKI service provider under the FICC's SSP program.

The AAIP staff formulated a detailed structured prototype process to evaluate the introduction and implementation of smart cards and PKI into the VA enterprise. During the prototype process, the project established a best practices system engineering approach where the technology was first tested in a controlled lab environment and then field tested at VA facilities. Examples include successful testing of AAIP and smart card usage for remote access over the enterprise gateways, integrated smart card log on at approximately ten separate locations across VA, and secure testing of smart card log on with wireless technologies, web access, database, and certain legacy devices.

The staff also established evaluation processes for physical access control systems and now serves as the central resource across VA as facilities plan efforts to move to the new federal GSC–IS standards based on the International Organization for Standards 14443.

VA is currently participating in the government's smart card aggregate buy of smart cards. Initially, VA will procure approximately 100,000 smart cards under the new Government Smart Card Interoperability Specification v2.1. This procurement is being managed by the General Services Administration pursuant to the guidelines from OMB. VA will start to receive these smart cards as early as October 2004. Part of the order includes new generation dual-physical antenna cards. At select facilities these cards will support coexistence with the current physical access control systems and the ability to migrate to physical access control systems that are compliant with the new GSC–IS specifications.

Finally, I believe VA has made great progress regarding this important effort, positioning ourselves to implement a smart card program ahead of the President's mandated schedule. I remain committed to implementing a smart card program that provides improved business functionality, increased security and enhanced services to our nation's veterans.

This concludes my oral statement. Thank you, Mr. Chairman, for the opportunity to discuss these important matters, and I'll be happy to answer any questions that you might have.

[The prepared statement of Mr. McFarland appears on p. 65.]

Mr. BUYER. Thank you, Secretary McFarland.

Secretary Brandewie, you're now recognized.

STATEMENT OF ROBERT J. BRANDEWIE

Mr. BRANDEWIE. Thank you, Mr. Chairman. Good morning.

Mr. BUYER. I'm sorry. I just promoted you. You're a Director.

Mr. BRANDEWIE. Director, yes. I am the Director of Defense Manpower Data Center. Our organization is responsible for the development, fielding, and maintenance of a number of DOD-wide information systems, including the DOD smart card initiative known as the Common Access Card, or CAC.

The Department began work in November of 1999 to modify the DOD identification card from a relatively low technology card to a smart card with an integrated circuit chip. The new smart card would be an authentication token for military members and employees and also contain Public Key Infrastructure, PKI cryptographic keys and certificates. This card would form the center of a strategic program to secure use of the Department of Defense network capabilities, and therefore it would increase security while at the same time enabling more efficient and effective web-based transactions for a variety of DOD business processes.

The initial test cards were produced in December of 2000, and full production of the new common access card began in September of 2001. By July of 2003, the full infrastructure was rolled out to 945 sites in 27 countries, and the program was fully implemented. Today more than 5.5 million CACs have been issued at the rate of more than 10,000 per day. Currently, about 3.2 million active duty and reserve military members, civilian employees and DOD contractors carry a valid CAC.

In addition to active duty and selected reserve members in the DOD, this includes Coast Guard members from the Department of Homeland Security, Public Health Service members in the Department of Health and Human Services, and National Oceanographic and Atmospheric Administration members in the Department of Commerce.

At the same time, and just as importantly, DOD has focused its efforts on improving the business process. A new DOD policy called Personnel Identity Protection requires strengthening of all aspects of credentialing DOD members and employees and authenticating those credentials before access is granted to DOD networks or DOD bases and buildings.

The process of performing secure, up front identity proofing and vetting is the foundation upon which a sound credentialing infrastructure is built. To this we add a very modern and secure issuance process. This issuance process is linked to the DOD enterprise central repository of affiliated people called the Defense Eligibility Enrollment Reporting System, or DEERS.

In addition, there are a number of procedures that strengthen the security of the issuance process. For example, we use only operators that have been favorable vetted by the Defense Security Service, and we require issuers of the ID card to be authenticated with their CAC, their PIN, and a biometric—a strong, three-factor authentication.

With regard to usage of the card, reforms in electronic business, paperless contracting, wide area workflow, travel re-engineering and expanded use of government-wide commercial purchase card programs have presented new opportunities to use smart card technology as an enabling tool for enhancing our business process.

In addition, the CAC is used for business applications such as a replacement for passwords or single sign-on, food service, deployment and warrior readiness, and manifesting. DMDC continues to work with the Components and other Defense agencies to develop more specific applications to enhance military readiness and improve the quality of life.

There has been a concerted effort to develop and use standards in the implementation of the CAC. The General Services Administration and the National Institute of Standards and Technology have been critical partners in this process. As a result, it is very easy for other agencies to adopt all or part of what DOD has done with the common access card.

DOD has worked and will continue to work with other federal agencies wanting assistance with similar programs or to provide information on valuable lessons learned. For example, DOD and the Department of Veterans Affairs have been in contact to share technical approaches to credentialing over the past 2 years. This continues with the announcement of Homeland Security Presidential Decision 12, which provides direction on a common identification standard for federal employees and contractors. Detailed meetings have been ongoing, including the meeting previously referred to today with representatives from all government agencies hosted by NIST.

DOD has been instrumental in the development of the current Government Smart Card Interoperability Standard, and the Department remains committed to working very hard with the existing tight deadlines to ensure a workable standard emerges to address HSPD–12's direction.

Thank you for the opportunity to address the Subcommittee. I would be happy to answer any questions.

[The prepared statement of Mr. Brandewie appears on p. 70.]

Mr. BUYER. Thank you very much. Mr. Pattinson, from your resume, you mentioned that you've worked with GSA, Treasury, Homeland Security, Veterans' Affairs and NASA. So given that sort of background, help me understand why interoperability is such a challenge, if that's our goal?

Mr. PATTINSON. First of all, identity management is a very complex subject. Any agency, any employee has generally many identities that they're using on a day-to-day basis. Putting an identity management system in place within an organization tries to aggregate all of those into a single identity and manage that through the access of all of those systems and services.

Each agency, each company have different and disparate systems. They're not all the same. There are different life cycles, different periods of time, different technologies. So even just putting an identity management system in is a complex task. Interoperability between agencies is even harder. This is because you've got the dimension of the further systems that are used in different agencies, again, all of their own volition, having to now move towards a stronger identity management within their own agency.

This is a hard topic. Interoperability is not easy. The work of NIST through the GSC–IS has been paramount in trying to pull together interoperability. Existing systems are migrating towards that, and as with HSPD–12, that will now create a framework and an umbrella for all of the future systems now to work together.

What's very important is common data. If you have different data in different places in the smart card or in the object areas of the smart card, you're not going to be interoperable. You have to have defined data, and defined ways of accessing that data so that therefore one agency's credential can be read and understood by another agency's credentialing system. If you don't have those standards, interoperability becomes extremely difficult to achieve.

Mr. BUYER. Were there any defects that had to be analyzed with regard to security for these cards?

Mr. PATTINSON. We've spent 25 years making smart ID cards. There are over 3 billion cards produced by our company worldwide. The security of the cards is in many forms, right down to the very specialized semiconductor chips.

They're not typical chips that you'd find in your home computer. These are very highly secure, specialized microprocessors designed specifically to be the local security agent in the hands of the cardholder on behalf of the issuer. They have to withstand attacks, tricks that people try to do to them from a physical perspective, from an electronic perspective. We have spent many years and the industry as a whole has perfected many, many hundreds of countermeasures within every smart card that we've produced that defends itself rigorously against attacks.

So we feel very confident that the combination of the two or three technologies that are being used by the Veterans' Affairs program are going to work very well for the needs of their applications. They have a legacy system of RFID technology for physical access. That clearly is being considered to migrate as they look at the three-chip card. I support the existing system and migrating over time to the newer, more secure physical access system using the second antenna.

The contact chip is the heart of the credential today used for Public Key Infrastructure, and those, as Mr. Brandewie has shown, are in full use within the Department of Defense providing very strong credentialing.

Mr. BUYER. Well, I asked that question as a follow-up to Ms. Hooley's question of the last panel. Let me ask, have you ever had to implement any countermeasures that you just mentioned?

Mr. PATTINSON. We have implemented hundreds of countermeasures in those cards. We have rigorously kept ahead of the attacks and people who are trying to——

Mr. BUYER. And who are doing the attacks?

Mr. PATTINSON. We find them to be all people from all places. A lot of university students like to write theses and show what they can do to try and attack the card. Often their attacks are not actually on smart card chips, they're on similar chips but claim to be smart card chips. They try attacking biometric technologies. We've seen various attempts at trying to defraud a biometric technology.

We try and keep ahead and looking at all of the things we can bring to bear from the physical side, from the logical side, to counter all of these attacks. This is our business. We are in the business of security.

Mr. BUYER. Now you were in charge of the security at the Winter Olympics in Salt Lake City. Is that correct?

Mr. PATTINSON. Axalto previously was part of Schlumberger, and yes, we were part of the Salt Lake City——

Mr. BUYER. Were there any problems with regard to the use of these cards at the Olympics?

Mr. PATTINSON. I'm not aware of there being any problems. It was a very comprehensive IT infrastructure to bring together all of the systems and mechanisms within the running of that facility. As far as I'm aware, it was an extremely successful implementation.

Mr. BUYER. All right. I have a whole series of questions, but I'll yield at this time to Ms. Hooley.

Ms. HOOLEY. Thank you. I have a question for Secretary McFarland. It looks like, at least by your report, that the project is on track, you're ahead, you're leading the way. What are the potential problems or trip points and what is being done to avoid those? What are you doing to avoid those?

Mr. MCFARLAND. Well, I have a strong belief that all projects need strong project management, and that to me is the first key. The second key is a realistic schedule, and along with that, buy-in from all the entities within VA on that schedule. The VA has approximately 225,000 employees with another couple of hundred thousand contractors and volunteers. It's around 500,000 people that we'll have to involve in this process over the lifespan. Without having complete collaboration with every facility out there, we won't do this on time. So I think we've done a very good job up front.

I truly commend the various administrations for buying into this project, because I think that's critical to the success of it. Each of them has unique facility issues that they have to deal with, and I think this project, as they well know, will solve some of those unique problems they deal with on a daily basis.

So I think the schedule is important and I think collaboration in getting the project off the ground and good project management will be the keys to making it happen.

Ms. HOOLEY. Tell me again what you do at the front end to make sure that the person you're giving this card to is really that person.

Mr. MCFARLAND. Well, I'll defer to Mr. Cadenas here, who really runs the project, to give you some idea of exactly what exhaustive things we go through.

Ms. HOOLEY. Thanks.

Mr. CADENAS. Good morning, ma'am.

Ms. HOOLEY. Good morning.

Mr. CADENAS. As Mr. McFarland said earlier, part of our effort is the level of collaboration. And as part of that collaboration, we actually work with the physical security entities within VA as well as HR, our Human Resources, and the local sites, including the administrators and law enforcement police there, because there's a number of checks that we do.

Depending on the user and his or her profile, we gather information, or we can gather information from various points. And in the case of VA, we plan on leveraging the existing infrastructure and working with the physical law enforcement personnel, since they are currently issuing cards or badges at this time. We will collaborate with them so they can issue a smart card that provides both physical access to facilities and logical access to systems and data. We will review the user profile to determine the level of access to systems and data. The law enforcement team will use the profile to determine the level of physical access as far as facilities.

So we have a number of checks and balances that we're doing to ensure that, one, the person is who he says he is. Then we do another check to see if the individual has any additional background or security clearance requirements, or needs physical access and logical access based on that user profile from a need-to-know point of view.

Ms. HOOLEY. Thank you. Mr. McFarland, in October 2002, the Secretary modified the control of the CIO. A large component of this project relates to information technology. Do you have adequate authority to meet any challenges that arise coordinating this project, and how far does this direct line authority extend?

Mr. MCFARLAND. I believe I have full authority to implement this project. This has been a project that has gone through our Enterprise Information Technology Board process, through a milestone environment where every administration and every staff office has had to participate in that environment. VA was working on this project long before I got here.

There were some things that I noticed when I came here that I made some modifications on, and those have all been vetted through all of the administrations and the staff offices. The Deputy Secretary has reviewed this project. The Secretary is aware of this project. I believe that we do not have any issues about authority or my ability to run this project to its end.

Ms. HOOLEY. By the way, congratulations. I mean, a lot of times we're always asking, why didn't you do this, how come you didn't do this, how come you're behind. It's nice to be able to sit here and say congratulations for being ahead of the game. Thanks.

Mr. MCFARLAND. Thank you, ma'am.

Mr. BUYER. Mr. Boozman?

Mr. BOOZMAN. Yes. I've been told that one of the test sites will be the Fayetteville VA hospital in Arkansas. Is that correct?

Mr. MCFARLAND. That's correct, sir.

Mr. BOOZMAN. Can you tell me a little bit about how that's progressing? You know, what the plan is, what exactly the cards will be doing there, what we're trying to get accomplished? I represent that district.

Mr. MCFARLAND. Yes, sir. I'll defer to Mr. Cadenas, who has the actual rollout environment there or can at least talk a little bit about the rollout environment.

Mr. CADENAS. Excuse me. I'm looking for the information. I'll be talking off the top of my head. What we plan on doing when we go down there, sir, is the reason why VHA identified Fayetteville as part of our effort with working with VHA, they identified that as a good sampling of a facility, if you will, within the VHA infrastructure. And because of the size and the scope and the things that we would like to test during the limited rollout, we thought we would be getting a very good exercise or a very good representation within a given month of this effort going on.

The first effort when we go to Fayetteville as part of the dry run will be working with the law enforcement staff there. We will be going through the actual process and we'll be issuing smart cards to address physical access. It's pretty much to do a dry run, and we're going to be doing it for a month. And I believe it's going to be up to a thousand cards. And then after that one-month trial run, we're going to sit down as a team with the VA community and review lessons learned, identify the potential risks and how we can mitigate those risks in the future, and see what other potential problems we could possibly encounter at the next site and address those before we actually move forward.

Mr. BOOZMAN. Well, I think it's an excellent choice. That VA hospital is run very, very well. And again, I think they'll be able to give you some good information. So anything I can do to help, be sure and let me know. Thank you.

Mr. BUYER. Secretary McFarland, you said that the CIO is in charge of all smart card projects. Is that correct?

Mr. MCFARLAND. That is correct, sir. And this project is the only smart card project we have active in the VA at this time.

Mr. BUYER. What about the swipe card project at Miami VA Medical Center involving physicians? Are you in charge of that project, also?

Mr. MCFARLAND. No, sir, I am not in charge of that project. It's under the auspices of VHA, but I can tell you that it is not a smart card project. It's a proximity card project, and it does not have the same technology involved in it. It is a test that was run along with, as far as I can determine, four or five other tests over the last few years, but it is purely a test. It's actually a project that only has six——

Mr. BUYER. Can I ask this? All right. If it's a proximity card——

Mr. MCFARLAND. A physical access card.

Mr. BUYER (continuing). Whatever that means, a proximity card, is it possible that when you do—and I understand what you're trying to do. We're trying to get a hold on the issue of physicians, their coming and going. And I also understand that when they implemented that project down there, you had two physicians who retired, two physicians who quit, and another one went to intermittent, out of the 60 physicians that are coming and going down there. You know, it's accountability. And I understand the VA is trying to get a hold of that, but is it possible that when you issue the smart cards that you also can include in your smart card your proximity card?

Mr. MCFARLAND. Absolutely, sir. Not only can we——

Mr. BUYER. And is that what you're thinking of doing?

Mr. MCFARLAND. Absolutely. Our intention is to replace those cards with smart cards and be able to do the same application environment they are currently doing there. We have no intention of having more than one card to get these processes done throughout VA.

Mr. BUYER. Okay. Good. You go to the VA just like all of us go to a VA, and they've got the chain around their neck. It's almost like a status thing—I got seven cards. (Laughter.)

You know. You don't need seven cards.

Mr. MCFARLAND. No, sir.

Mr. BUYER. Right? We don't need all of that. So you're going to be in charge of the smart card. You know what the other side is doing out there, and you're going to try to incorporate that, and this is just a pilot. We don't expect this to be going on at other places, right?

Mr. MCFARLAND. No, sir. That is the only place those 60 cards are issued, and there is no intention of putting those cards in any other environment. When we get into the Miami facility, we will replace those cards with the smart card technology we're implementing in the rest of VA.

Mr. BUYER. All right. When there are breaches of security, can you tell me whether or not there have been disciplinary actions taken for breaches of security? I mean, is this happening out there? If this question is outside your lane, just tell me. But are you aware when there are breaches, security breaches of information systems, major security breaches?

Mr. MCFARLAND. Yes, sir. I am aware whenever there are breaches in the information security system. I can't comment on breaches of security of physical access and facilities. That would fall under law enforcement, as I understand it.

As far as breaches in information security, that's what cyber security is about in the VA. It is the single point of security for all of our cyber environment. And over the last year, year and a half, the VA has rallied around cyber security to be the single point of contact there. So I believe that through our Central Incident Response Capability (CIRC) process, we are aware of all of the information security violations that we can detect and that have been reported to us. There is still a very large information security administration out in the VA with as many facilities as we have, and we have some 200 Information Security Officers out there. We rely on them to give us as much information as we can get, and we most often do find out immediately when there's a violation of cyber security.

Mr. BUYER. And who is going to be primarily responsible for the issuing of the new smart card?

Mr. MCFARLAND. Primarily responsible for issuing of the smart cards?

Mr. BUYER. Yes.

Mr. MCFARLAND. Cyber security is running this project. AAIP is under VA's cyber security office.

Mr. BUYER. Is that you? Who——

Mr. MCFARLAND. Mr. Baffa.

Mr. BUYER. Where is he?

Mr. MCFARLAND. Right over there.

Mr. BUYER. Who is Baffa?

Mr. BAFFA. I'm Baffa, sir.

Mr. BUYER. And you're law enforcement?

Mr. BAFFA. Yes, sir. Physical law enforcement, yes, sir.

Mr. BUYER. Fiscal law enforcement? Come over to the podium for just a second.

Mr. BAFFA. Yes, sir.

Mr. BUYER. You have physical security?

Mr. BAFFA. Yes, sir, I do.

Mr. BUYER. For law enforcement?

Mr. BAFFA. Yes, sir.

Mr. BUYER. And Mr. Cadenas, you're going to be the one responsible for the issuing of the cards?

Mr. CADENAS. We address logical security, as I said earlier, sir; this is where it's a team effort to leverage the existing infrastructure out there that's doing the work today.

We are working with Mr. Baffa and his organization to identify the equipment, the training, policies, and procedures that what we're going to do, sir, is when we're on the ground, we're going to be working with his law enforcement staff since they currently are doing badging at all the facilities or clinics.

And what we're going to do, sir, is when we pull that old technology out and we put in the new smart card One VA community card, we will train and work with the local law enforcement staff, provide the equipment as close to a turn key solution, so it becomes very transparent to them, old system out, new system in. We still issue the physical card or the physical access card and ID badge. And on top of that, because of our relationship, then we will come in and ensure that the logical profile of the user is addressed within that card, if you will, one-stop shopping for everything.

Mr. BUYER. Sir, will you state your name?

Mr. BAFFA. Yes, sir. My name is John H. Baffa.

Mr. BUYER. And your title?

Mr. BAFFA. Deputy Assistant Secretary for Security and Law Enforcement.

Mr. BUYER. And will you please tell us how—your plans to implement the smart card on the ground through law enforcement? You have physical security?

Mr. BAFFA. Right. You know, we're taking—the concept that you alluded to, going to a VA hospital, a person may have one to six to seven cards around their neck, what the smart card is going to do, and you also heard about proximity cards and swipe cards, is replace all of them.

What the smart card will do is going to really—it's going to envelop everything. It's going to take the physical security aspect which you will need your smart card, as today you need this card in the VA to get to certain areas. It's going to not only act as a cover for physical but also for computer security, it's going to all be intertwined.

We will be the ones responsible for ensuring this. This is a very simplistic way of saying it from the physical security aspect all we're doing is trading the smart card for a card that we already have and we use for identification, recognition, et cetera. But within that, with the computer technology, we'll have both the physical and computer security bases covered, or we believe we will.

Mr. BUYER. And do you have good cooperation from union leadership? They've been briefed on this?

Mr. BAFFA. I'll have to defer that.

Mr. CADENAS. Yes, sir, they have, and we were—the reply back from them, they were very pleased that we had been working with them and the fact that we brought it up to their attention early on, and we have not had any negative comments or concerns at this time.

Mr. BUYER. So if I'm an employee and my smart card will ensure that I have access to particular areas, it's going to, by virtue of my position, that would be programmed into the card?

Mr. BAFFA. That's correct.

Mr. CADENAS. Yes, sir, your user profile, if you will.

Mr. BAFFA. From the physical and computer aspect, that's correct.

Mr. BUYER. Oh, I like that.

Mr. BAFFA. And I'll be able to know if you were there, basically. It'll have a tracking device.

Mr. BUYER. You lose sort of this stigma thing that's going on out there, too—"I'm more important than you" kind of thing with all these cards.

Mr. BAFFA. I agree with you.

Mr. BUYER. It is. It's kind of a status thing. It's ridiculous that's going on.

What about the photos? We can't use our high school photos, right?

(Laughter.)

Mr. BAFFA. No, sir, you can't. The photos like in central office, if I should forget to bring my card in and I go to the main desk of the guard and I say I'm John Baffa, the first thing I have to do is to show him my driver's license. That's the first verification. Then they'll hit the name in the computer, and this pass will come up on the computer screen to verify who I am. And that's the posture we would take at the local facilities, also.

Mr. BUYER. That's great. Remain there at the podium. Let me yield to my colleagues for any questions they may have based off any of these. You're fine? All right.

Do you anticipate any problems out there that you've got groups working on that we should know about?

Mr. BAFFA. No, I think, there may be some growing pains, and that's why we're doing the pilot site, and I believe we're starting with VISN 16. We're going to try and stay in one part of the country initially, and we have various sized facilities there. No, I don't think—you know, the one thing I think that has to be clear, though, is during this transitionary period when you go to Miami or wherever you go to, there will be two cards. We'll have the old card plus the new smart card till we make sure that the physical access security systems in place can be interloped with the new smart card. So there will be a short period of time where you will be required to wear two cards. But eventually, once this whole process is completed, this thing will get you into the building, get you into the area that you need to, and conversely, keep you out of areas you don't need to be in. And then, as I said, we'll know where you've been.

Mr. BUYER. All right. Thank you very much.

Mr. BAFFA. Yes, sir.

Mr. BUYER. Ms. Hooley, do you have any other questions?

Ms. HOOLEY. No, I don't.

Mr. BUYER. Do you have any other questions? I do for Mr. Brandewie. You may have a seat. Thank you, sir.

Mr. BAFFA. Thank you.

Mr. BUYER. I appreciate it. When you did your rollout of your smart cards for DOD, did you have any difficulties?

Mr. BRANDEWIE. Well, yes, sir. I mean, the model that we used to issue the cards is a decentralized one, so we had to put card issuing stations all over the world. So it took a while to deploy the issuance facilities. But today we issue cards, for example, in Iraq, and in 26 or so other countries over the networks, including PKI credentials.

So we've essentially overcome a lot of the initial technical problems and have a stable environment now and a stable infrastructure for issuance of the cards.

Mr. BUYER. With any card, as with any key, it's all about control. Without biometrics, how do we ensure that security, that someone can't program that card for access? I'd like for you to answer, and then I definitely—I was looking at Mr. Pattinson. Go ahead.

Mr. BRANDEWIE. We do incorporate biometrics, sir, in our system, in our issuance system. So, for example, before we reissue a common access card or issue a common access card, we have a biometric authentication that's done with a member who's attempting to get a new card. We biometrically authenticate them, as well as do a—look at the picture that's stored in the system and make sure it's the same person.

So we have biometrics deployed throughout the Department and have been collecting biometrics since 1996, but it's not yet on the card. And the not yet on the card is because standards are just emerging for the use of interoperable biometrics on the smart card. But biometrics are in our infrastructure, just not yet on the smart card.

Mr. BUYER. And is the only err then of the system would like with the custodians? And of a size of a DOD, the custodians out there of that—there's got to be a large number, right?

Mr. BRANDEWIE. Of the issuance process?

Mr. BUYER. Yes.

Mr. BRANDEWIE. Yes. We have about 5,000 people in the—that are we call verifying officials. These verifying officials are the issuers of the card. But as I mentioned in my testimony, they are vetted by DSS, so they have to go through a national agency check process. And then we biometrically authenticate them with a fingerprint. We also require the CAC to be present, and we also require them to use their PIN to issue the card.

Mr. BUYER. Is there any convergence, military ID card, smart card, health record, too much information on a card?

Mr. BRANDEWIE. The plan, the data plan for DOD, was not to put a lot of data on the card. In fact, we limit the amount of personal data on the card to the bare minimum necessary, simply because we want the card to be an authentication token of identity and not a data carrier.

The data resides in central systems, and the card becomes a proxy for identity, and the central systems have the detailed data. The problem——

Mr. BUYER. So in the military we're going to have two cards?

Mr. BRANDEWIE. No, sir. The common access card is the military ID card. Its smart chip carries personal information. It's the Geneva Convention card and the military ID card.

Mr. BUYER. Okay.

Mr. BRANDEWIE. A single card for all active, reserve, civilian and contractor personnel within the Department.

Mr. BUYER. All right. All right. I'm with you. I had a hiccup there. It's with our dog tags that we'll then do our medical records, right? So we're kind of carrying two cards.

Mr. BRANDEWIE. Yes, sir.

Mr. BUYER. All right. Mr. Pattinson, you had comments.

Mr. PATTINSON. Certainly. I wanted to address the comment about reprogramming a smart card. I want to show you that our business of making smart cards is around making them extremely difficult to reprogram by anybody who shouldn't be doing that.

We provide a comprehensive technology to do with cryptographic keys and access to the smart card content that only the issuer of the card can get access to, and thereby, the card cannot be reprogrammed.

With regard to biometrics, the smart card offers extremely comprehensive capability of either providing biometric template information to an external piece of equipment for biometric matching, or in more advanced use, it can perform that operation within the smart card device itself, so the biometric template can be captured and presented to the smart card. The smart card can be that security agent on behalf of the issuer to match the biometric within the card and provide a secure answer that yes or no, this is the correct cardholder. This card belongs to me or not.

And I really believe that that use of matching card technology is a very strong addition to much higher forms of authenticated identity by using the smart card technology.

The TWIK program that's currently under discussion within the Transportation Security Administration is looking very strongly at biometrics for identification at enrollment, and secondly then for biometrics for use for user authentication in the use. They may not be the same biometric. One is to do a one to many match to verify if they have a criminal background or are already enrolled. The second is for verifying that this card belongs to me now. Thank you.

Mr. BUYER. Mr. Pattinson, I want to thank you for your leadership and your contribution on this. You've spent a lot of years in this area, and I appreciate it. I also want to compliment your work at the Olympics. You know, sometimes when you work hard and things go well, you get no attention. And so, congratulations on a job well done.

Mr. PATTINSON. Thank you, Mr. Chairman.

Mr. BUYER. I have two questions sort of unrelated, Secretary McFarland, and then I have a question for you, Mr. Brandewie, also unrelated. I'd like to know what the status is of the CoreFLS debacle at Bay Pines. I understand the Department is going to attempt to recoup a fraction of the millions paid to the contractor. If you could comment on that, I'd like to know the status and whether or not you've made any decision about what to do with the program.

Mr. MCFARLAND. Well, sir, currently, as of October 1, the three test sites, Bay Pines, the national cemetery in Tampa, and the St. Louis BVA Regional Office, have all converted from CoreFLS back to the Financial Management System (FMS), which is the system the rest of VA is running on. They will begin to accept financial transactions on October 8, the same date that all of VA will begin accepting new fiscal year transactions.

That conversion has gone, as best as I can see, very well. I'm actually very happy and surprised we got back as easily as we did. I shouldn't use the word "easily." There are among people who put a lot of time and effort in that, so we could get back in the timeframe that we did. And VHA is to be commended for really aggressively attacking that issue and getting back.

As for CoreFLS, first off, we will continue maintaining all the licensing of the products that we have. We have no intention of throwing those away. One of the products, DynaMed, will continue to be used and is in use at Bay Pines. The original generic inventory package was not installed there, if you remember, before we started that project. And we will be continuing with the DynaMed inventory package and looking at that from the standpoint of how it fits in that large hospital environment so that we can see how it might fit in other parts of VA. I applaud that. I think it's a good use of the product, and I think we'll have some good knowledge to compare with our other inventory packages as to how well that package will work.

We will also maintain in the Austin Automation Center a CoreFLS data warehouse. I've scaled it down dramatically from a cost standpoint from where it was. But we want that data available in case we need to go back into fiscal year 2004 transactions for any of those three sites and confirm data or pull data that we didn't get converted over or we didn't see a need to convert over. So we'll have that still running. That's going to be running in the Austin Automation Center on a scaled-down basis.

The rest of CoreFLS is under what I would call a lights-out environment for the time being. In other words, we won't be actively running the applications of CoreFLS anywhere else. The process of going forward is now in the works. The Secretary has put together a board of directors which I head up. The Board is looking at the go forward strategy. We've had some significant meetings. We're gathering lessons learned. I have put out a contract for an IV&V with Carnegie Mellon.

Mr. BUYER. For a what?

Mr. MCFARLAND. An IV&V, which is an Independent Verification and Validation contract, to get Carnegie Mellon to take the study they did and deliver back to us the lessons learned from all of the data they gathered in that project that we gave them originally.

We're also going to be setting up an internal VA lessons learned environment so anyone involved in this project will be able to share opinions and lessons learned. That way we can gather the in-house knowledge as well as the out-of-VA knowledge.

We're then going to get some professional help in looking at where we go forward with our strategy, understanding our as-is environment and looking at what we do to go back again and realize how we can mitigate these problems of the material weaknesses we had in our financial and logistics systems.

I'm pretty confident that if we take this process slowly and methodically this time, that we can find where we need to go and what we need to do to solve those weaknesses.

Mr. BUYER. All right. The question was out of scope. If minority counsel has any follow-up based off that question, it's permitted. The other question deals with I'd like a status check on the third-party collections demo in Cleveland, the PFSS demo. Is it alive and well? Is it on life support? Does it need to be resuscitated? Is it systems go? What is it?

Mr. MCFARLAND. Well, I was there last Monday and got my first demonstration of the IDX product, which is the large piece of that project. I got a full understanding of the implementation plan. Although I don't have the data with me, I can tell you that I was pretty impressed with the product, to be honest with you. It will give the VA a tremendous amount of capability to capture this information that we need to bill and to track that information. One of the things I was most impressed with is when data isn't gathered, you can't get out of the system until you answer the questions and until you get the data. It doesn't go away, which to me is a significant advantage.

I reviewed with the project team and with Unisys where we are on the project. I came back and reviewed VHA's part with Dr. Kolodner, the Acting Deputy CIO for Health, to make sure that we are on track with the piece that VHA is doing. So far, we are on schedule.

I also spent some time with the project manager there, the VA project manager, and was impressed with her ability to ramrod the project. So I came away pretty bullish. And as you know, two weeks ago, I was not so bullish. I think the proof is in the pudding. We have to execute on this. But so far, I think we're on track.

Mr. BUYER. Last time we were here, we talked about putting some competition out there in the marketplace and we the government, i.e., the VA is going to benefit from that. Can you give us an update as to whether or not that's feasible? And if so, you know, we have a few weeks to actually make that a reality here in the Omnibus Bill and negotiate this out with Chairman Walsh. So, can you give this committee an update?

Mr. MCFARLAND. Well, I'm in agreement with you that we have an awful lot of facilities that need this help, and the Patient Financial Services System (PFSS), as good as it can be and will be, is not going to get all those facilities up and running in the near term. So I'm anxious to see what we can do about some contributing technologies that can do the same kinds of things, through this committee's help.

We reviewed a company just this week, earlier in the week, that has some capability in doing the kind of things that PFSS is designed to do. Ken Ruyle and I both attended that presentation. We both came away believing that we think we might have some ability to run a parallel process. We're investigating the possibility of doing that.

I think unless there are some things we don't know, we might be able to find a facility that we can run a parallel situation. I did not come away with a good handle on costs, and I need to ask a lot more questions about how we would do this. I also need to figure out how we could manage more than one project at one time, and so I want to be sure we do that.

Mr. BUYER. We would obviously need that input.

Mr. MCFARLAND. Right.

Mr. BUYER. You know, we're pretty concerned about how Unisys got this contract, and it's one that has just grown exponentially, and so we're a little concerned about that, and that's why we initiated this conversation with you. And at the same time, we don't want to overburden you in the management of two tests. But at the same time, having that competition out there is going to be healthy and maybe cause some restraint.

But you need to give us a bogey. You need to tell us what that number is over a period of time. Give me a timeline. Let me know what the number is, and this committee can work with Chairman Walsh, and maybe this can be made a reality.

Mr. MCFARLAND. We will certainly investigate that.

Mr. BUYER. I don't have a lot of time.

Mr. MCFARLAND. I understand that, sir.

Mr. BUYER. I mean, when you look at when this—you know, it's not a lot of time, all right?

Mr. MCFARLAND. I understand.

Mr. BUYER. Okay.

Mr. MCFARLAND. And we are moving as aggressively as we can to determine what it would take to put another test in place.

Mr. BUYER. Well, good. I look forward to a follow-up conversation with you then.

Mr. MCFARLAND. Yes, sir.

Mr. BUYER. Mr. Brandewie, Do you have any follow-up questions based on that out of scope? Thank you. The last out-of-scope question deals with, Mr. Brandewie, you are intimate with something that's very personal to me. What I've learned about in Congress is if you create it, it's yours for life. It doesn't matter even it becomes something you don't like, it doesn't matter. It's yours for life. Mine's TRICARE for Life. If you author it, it's yours forever. And even though I wasn't there to implement it, I am—I've been impressed, and I've been disappointed. And so let me compliment you. This was very difficult and very challenging. The implementation of TRICARE for Life has been very meaningful to a lot of people out there, and I get those stories. And so I want to please convey that to you, the appreciation by many people.

I also am co-chair of the Guard and Reserve Caucus that we created years ago, so I also get to hear from the Guardsmen and the reservists and the dependents on difficulty in the access, and it's you, right?

Mr. BRANDEWIE. Yes, sir. The DEERS system is the gatekeeper for TRICARE.

Mr. BUYER. So can you tell me what I get to tell, what the committee gets to tell the sergeant that's been called up and the family is having their difficult problems getting into health care and why the lag? Can you help us out?

Mr. BRANDEWIE. I'd mention two things, sir, that I think are important in that regard. One has been the extremely difficult challenges of sorting out the activations between the guard/reserve components and the active duty components.

We've tried very hard since—obviously, the volume of activations has increased. We've tried very hard to put in place a process which smoothes that, that process. In fact, the Guard and reserve personnel systems are different than the active duty personnel systems, and it's that crossover that has been causing some of the problems you refer to.

In addition to that, we try to really adjust the timing of the benefit to the timing of the activation. Often that has proven challenging. People get extended, for example, in theater beyond their original orders. And so their eligibility for the benefit extends, and often we're behind the power curve in getting that information from the personnel systems and into DEERS.

There's a second issue, and that has been the implementation of the legislative authority that came out last year in the Defense Authorization Bill with respect to alerting—TRICARE eligibility for alerted Guardsmen and reservists. That has also proven challenging, since that information was outside the purview of DEERS, and we've had really a difficult time working with the services to get it into DEERS.

Those two issues I think have complicated the smooth operation of DEERS with respect to guardsmen and reservists. On the other hand, I would point out that we have a very active and available help facility for DEERS and TRICARE eligibility that's been used extremely extensively by Guard and reserve family members and the service members themselves. The volume is way up, but those people are expert in fixing the problems that have occurred out of this mismatch in the personnel systems.

And so we're using that technique to try and make this process more smooth, or smoother.

Mr. BUYER. You know, we could go across the Atlantic and go to the United Kingdom, and the United Kingdom takes their VA and it's under their Ministry of Defense sub-part, and they don't even break it—in the House of Commons, they don't even break that out, right? It all comes under their defense budgets and their oversight, and their veterans don't particularly like that, but that's what they do.

But guess what? They don't have problems with interoperability. They don't have problems with personnel systems, right? So here in our country, we've done this advocacy and we create "veterans are going to be their own," "we're going to have our own," by golly. We're our own. And then we end up with these tons and tons of problems. We can't even decide what the word "interoperable" means, right?

So, you know, look at the challenge, Secretary McFarland. You come from the private sector and you want to help your government. I congratulate you for that. But look at this. We take a reservist or a Guardsman that's just been activated, their dependents, they've got their own series of issues. I change the law to make sure that they—we waive their deductibles, we try to make it easy for them, right? So we bring them in. We've got a personnel system that has a hiccup, and oh, by the way, that health record which we're creating is not even accessible into the VA for which we may end up be receiving him when he's wounded or injured.

You know, that's why I'm going insane. Those are our challenges. Those are our challenges, and those are the things we've got to do. They're hard, and I know they're hard. But that's what we have to do. We're here to do the hard work, and that's why, Secretary McFarland, I really am proud of you, because you don't have to do this, and you're taking this on, and this committee has given you great latitude to get your arms around this one and to begin to exercise the authority.

And if you ever feel you don't have that authority, this committee, I've told you before, we're prepared to give you whatever budgetary authority is necessary. If it's not there in this next Congress, I think in a bipartisan fashion, we'll give it to you, all right? You just tell me.

This hearing is now concluded.

[Whereupon, at 11:24 a.m., the subcommittee was adjourned.]

APPENDIX

Statement of

Benjamin H. Wu

Assistant Secretary for Technology Policy Nominee
U.S. Department of Commerce

Before the

Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations

"Smart Card Activities of the
National Institute of Standards and Technology"

October 6, 2004

Chairman Buyer, Ranking Member Hooley, Members of the Subcommittee, thank you for this opportunity to testify today about the National Institute of Standards and Technology's (NIST) activities related to the advancement of smart card and biometric technologies within the Federal government. You are to be commended for your leadership to implement smart card technology at the Department of Veterans' Affairs. NIST plays an important role in cooperation with other Federal agencies, to eliminate the road blocks to widespread deployment of smart cards. As part of the Department of Commerce's Technology Administration, NIST is working with industry and other government agencies to provide interoperability specifications, standards, and guidelines with the goal of expediting open and interoperable methods for using smart cards. NIST will be leading the President's assignments to the Department of Commerce required by the Homeland Security Presidential Directive/Hspd-12, "Policy for a Common Identification Standard for Federal Employees and Contractors." NIST has also done considerable work in the area of biometrics under the auspices of the USA Patriot Act.

Background

Smart cards provide opportunities for improving security of our critical infrastructure, both from a physical and logical perspective. Because they are capable of performing cryptographic functions, they can perform important security services such as securely storing digital signatures, holding public key credentials, and authenticating a claimed identity based on biometric data. As such, smart cards are a crucial element in a range of current and expected critical applications and programs. They are also the underlying foundation for the standard required by Hspd-12.

NIST's smart card program dates back to 1988. Recognizing the potential for smart cards to improve the security of Federal IT systems and our national information infrastructure, NIST chose to invest significant research effort in smart card technology at an early stage. The NIST smart card program produced many early innovations in the area such as a generic authentication interface for smart cards, the first cards to implement the Data Encryption Algorithm and the Digital Signature Algorithm, and the first reprogrammable smart card. These innovations are integral to modern smart cards.

Many Federal agencies have a longstanding interest in smart card technology. However, large-scale deployment of smart cards has proven challenging. A survey revealed that agencies found it difficult to deploy large-scale smart card systems due to a lack of interoperability among different types of smart cards and without assurances of interoperability, agencies would be "locked" into a single vendor. Thus, the issue of interoperability had to be addressed before significant investments were made. Additionally, smart card systems have historically been driven by requirements arising from specific application domains such as banking, telecommunications, and health care. This has led to the development of smart cards that are customized to the specific application requirements of each domain, with little interoperability between domains. These vertically-structured smart card systems are expensive, difficult to maintain, and often based on proprietary technology.

GSA created a contract vehicle and program to procure interoperable smart card systems and services and to promote and facilitate the use of this critical security technology within the Federal sector. After much work to address the Federal customer needs identified, NIST published two versions of the Government Smart-Card Interoperability Specification in June 2002 and July 2003, respectively. (Available via http://smartcard.nist.gov/ .)

The GSC-IS has been well received and is making a significant impact. Many Federal agencies are moving forward with plans to deploy large numbers of GSC-compliant systems. The Department of Defense's Defense Manpower Data Center, Common Access Card (CAC) Program Office has stated the following about NIST and smart cards:

> *Our department recognizes the ...technical skill and leadership in the area of Smart Card Interoperability and building the Government Smart Card Interoperability Specification... vital to the interests of our Department as well as a major contribution in the Federal Sector regarding national security.*

DoD has adopted the Interoperability Specification for their enterprise-wide CAC deployment, representing millions of cards (to be effective in 2004.)

Standardization

GSA and other Federal agencies have long sought to avoid the problem of being locked into proprietary, non-interoperable smart card technologies. Recognizing the needs of the Federal customer base, NIST is working with American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) to standardize this specification. ANSI carried a new work item to ISO that was based on the NIST smart card work. This new work item was balloted and overwhelmingly approved by the national bodies. Of the 24 countries voting, 19 voted yes, two did not cast a vote, and two votes were qualified no's that later changed to 'yes'. An international task force has been established, with NIST as the chair. The work of this task force is to develop a new suite of smart card interoperability standard, which are based on NIST IR 6887 – Government Smart Card Interoperability Specification. This Task Force was established in April of 2004 and has already met twice, has a new work programme approved, has been given an ISO number for this new suite of standards, (ISO 24727) and is scheduled to provide drafts in March of 2005. The Task Force has the backing of the international community and is moving very aggressively and plans to have approved standards within 24 months, which is very aggressive for an international effort.

Additionally, ANSI has established a new national work group to address national smart card interoperability standards work. This group is chaired by NIST.

In summary, in the last 11 months NIST has successfully accomplished significant steps in the formal standards world by being the leading and driving force in 1) the establishment of a formal ANSI Task Group to address smart card interoperability at a National level, 2) the overwhelming approval for a new international standard and 3) the establishment of an international Task Force, with support to Chair this new group.

The Government Accountability Office (GAO) issued a report in January 2003 on the Federal government's progress in adopting smart card technology. The report stated:

> *We recommend that the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies – such as contactless, biometrics, and optical stripe media – as well as integration with PKI, to ensure broad interoperability among Federal agency systems.*

In response to these GAO recommendations and identified Federal agency needs, NIST is examining requirements for and issues associated with definition of a multi-technology card platform. Technologies being investigated for utility in a multi-technology platform include smart card integrated circuits, optical stripe media, bar codes, magnetic stripes, photographs, and holograms. As a first step, NIST hosted a workshop on multi technology card issues in July of this year. The workshop focused on requirements, issues, and Federal government activities associated with multi-technology cards. More specifically, it examined general technical and business issues, existing voluntary industry consensus standards, gap areas in standards coverage, and industry capabilities in the field of ISO/IEC 7810-compliant storage and processor card technologies. The workshop also addressed multi technology integration issues, and both inter-jurisdictional and inter-technology interoperability issues.

Based on the proceedings of the workshop and subsequent interviews conducted with the user community, NIST produced a technical report that identified integration and interoperability research topics, gaps in standards coverage, and multi-technology composition issues. This was completed in March 2004.

NIST published the GSC-IS, Version 2.1 in July 2003 as NISTIR 6887, 2003 Edition. This document addresses the remaining GAO recommendations by providing support for biometrics, contactless smart card technology, and Public Key Infrastructure.

There is considerable interest in the convergence of biometrics and smart cards. In response to requirements from the GSC customer base and recommendations in the GAO Report, NIST has included 'hooks' for biometric authentication modules in Version 2.1 of the GSC Interoperability Specification. During FY03, NIST also worked with an ANSI M1 ad hoc group to publish an analysis of existing biometric and smart card interoperability standards with respect to their ability to support integrated smart card-biometric systems. The report includes detailed recommendations for designing a GSC biometric plug-in framework. It has been submitted to ANSI B10 to provide a roadmap for integrating full biometric capabilities into the GSC framework during the formal standards development process. Published August 2003, the report is available to the general public on the ANSI/INCITS M1 document register (http://www.incits.org/tc_home/m1htm/docs/m1030398.pdf.).

Moreover, NIST is actively working with Europe and Japan towards a general smart card framework that can harmonize and align a variety of disparate approaches, technologies, and architectures. We believe that this would yield greater interoperability, lower costs and barriers, and enhanced security.

Smart Card Conformance Testing

Conformance testing is an important and integral element of a standards program. It can increase the confidence for consumers that a given product does conform to a given specification reducing the risk to the purchaser. NIST has been developing an interoperability conformance test program in parallel with the GSC standards effort. The GSC conformance test program will rely on commercial laboratories to validate conformant products, providing customers with increased assurance that these products meet the interoperability requirements of the GSC framework. NIST conformance test engineers and programmers are developing test criteria and building a suite of conformance test tools to be used by commercial laboratories to test and ultimately improve private-sector smart card products.

Homeland Security Presidential Directive -12

Hspd-12 was issued on August 27th, 2004. The directive calls for the Secretary of Commerce to issue a Federal standard for secure and reliable forms of identification (ID) issued by the Federal Government to its employees and contractors (including contractor employees). This standard will serve as the basis for the creation of a secure and reliable ID that, 1) is issued based on sound criteria for verifying an individual employee's identity, 2) is strongly resistant to identity fraud, counterfeiting, and terrorist exploitation, 3) can be rapidly authenticated electronically and 4) is issued only by providers whose reliability has been established by an official accreditation process. The standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

This is obviously quite an ambitious assignment and one that will considerably aid the homeland security efforts of the Federal Government. While developing the standard required by Hspd-12, we will ensure that ample privacy protections are included.

Within the Technology Administration, NIST is taking the lead in developing this standard and has developed an ambitious timetable to meet the six-month deadline. NIST is working with the Office of Management and Budget and other departments and agencies to take advantage of efforts currently underway within the Federal Government.

NIST will also be working with the public and private sectors to develop the standard. Today, NIST is holding a workshop with over 80 Federal agency representatives to discuss the development of this standard. Additionally, tomorrow (October 7, 2004), NIST is holding a public workshop for industry and others to discuss its plans and to solicit ideas and feedback.

Further Research and Development

Smart cards and associated technologies hold great promise for meeting many important needs in homeland security. Success in large-scale deployments of smart cards and their associated applications, however, is not assured. As a community, we will have to be innovative in finding ways to fund and develop the needed tools, tests, examples, frameworks, best practices, and research to deliver scalable, secure, and interoperable smart card infrastructure and associated applications.

Some of these tasks include the development of reference implementations, software developer's toolkits, data models, issuance policies, credential management, publication of implementation guidance, pilot projects and continued research and development. An educational program to share information and avoid duplication of effort would be of great benefit as well. Most of the Federal agencies that comprise the GSC community have budgets for their own smart card deployments, but these budgets do not include support for an interagency research and development program. Developing standards is critical to ubiquitous adoption (and achieving the attendant security benefits) of smart cards, and this work will continue to be of great importance.

Summary

The U.S. GSC-IS has generated considerable interest and support in both the U.S. domestic and international smart card communities. By developing a viable commercial market place for smart card technology in the U.S., we can increase the competitiveness of the U.S. smart card industry in the global market, while improving the security of our nation's critical infrastructure. NIST is continuing to improve and update smart card interoperability specifications and actively participate in Federal coordinating efforts. The smart card work will also play a key role in developing Federal employee credentials required by Hspd-12.

I would be pleased to answer any questions you may have.

United States Government Accountability Office

GAO

Testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

For release on delivery
expected at 9:30 a.m. EDT
Wednesday, October 6, 2004

ELECTRONIC GOVERNMENT

Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs

Statement of Linda D. Koontz
Director, Information Management Issues

GAO
Accountability * Integrity * Reliability

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-84T, a testimony to the Subcommittee on Oversight and Investigations, House Committee on Veterans' Affairs

October 6, 2004

ELECTRONIC GOVERNMENT

Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs

Why GAO Did This Study

The federal government is interested in the use of smart cards—credit card-like devices that use integrated circuit chips to store and process data—for improving the security of its many physical and information assets. Besides providing better authentication of the identities of people accessing buildings and computer systems, smart cards offer a number of other potential benefits and uses, such as creating electronic passenger lists for deploying military personnel and tracking immunization and other medical records.

Over the past 2 years, GAO has studied and reported on the uses of smart cards across the federal government. The Subcommittee requested that GAO testify on federal agencies' efforts in adopting smart card technology—based on the results of this prior work—and on the specific actions that the Department of Veterans Affairs is taking to implement smart card technology.

www.gao.gov/cgi-bin/getrpt?GAO-05-84T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

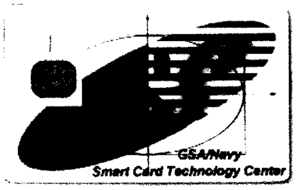
What GAO Found

As the unique properties and capabilities of smart cards have become more apparent, federal agencies, including the Office of Management and Budget, the National Institute of Standards and Technology, and the General Services Administration, have acted to advance the governmentwide adoption of smart card technology. In turn, numerous smart card projects that offer a variety of uses and benefits have been launched. As of June 2004, 15 federal agencies reported 34 ongoing smart card projects. Further, agencies' actions toward the adoption of smart cards continue to evolve as understanding of the technology grows. Agencies are moving away from the small-scale, limited-duration demonstration projects of past years (involving as few as 100 cardholders and aiming mostly to show the value of using smart cards for identification) to larger, more integrated, agencywide initiatives involving many thousands (or even millions) of users and that are focused on physical access to facilities and logical (information systems) access to computer systems and networks.

In pursuing smart card projects, federal agencies have had to contend with numerous management and technical challenges. However, these challenges may be less imposing in the future because of increased management concerns about securing federal facilities and because technical advances have improved the capabilities and cost effectiveness of smart card systems.

The Department of Veterans Affairs (VA) is one of 9 federal agencies currently pursuing large-scale, agencywide smart card initiatives. VA's project, currently in limited deployment, involves using, among other technologies, the One-VA Identification smart card to provide an agencywide capability to authenticate users with certainty and grant them access to information systems essential to accomplishing the agency's business functions. VA estimates that this project will cost about $162 million between 2004 and 2009, and enable it to issue 500,000 smart cards to its employees and contractors.

A Typical Smart Card (not to scale)



Source: GSA

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to participate in the Subcommittee's hearing regarding the adoption and use of smart card technology. Smart cards are plastic devices—about the size of a credit card—that generally use integrated circuit chips to store and process data, much like a computer. This processing capability distinguishes these cards from traditional magnetic stripe cards, which cannot process information interactively with automated information systems.

Our prior work has found that smart cards offer a variety of benefits to the federal government, such as better authentication of cardholders' identities, increased security over buildings, more effective safeguards of computer systems and data, and more accurate and efficient financial and nonfinancial transactions.[1] The General Services Administration (GSA) has promoted the adoption of smart card technology across government based on a goal of equipping all federal employees with a standardized smart card for a wide range of services. Nonetheless, the successful adoption of smart cards throughout the federal government has been a challenging task, and federal agencies' adoption of this technology continues to evolve.

At your request, my remarks today will summarize the federal government's efforts toward adopting smart card technology and the challenges that have been encountered. Also included in my discussion is an overview of the actions that the Department of Veterans Affairs (VA) is taking to implement smart cards. In addressing these objectives and developing this testimony, we relied primarily on previously reported information describing federal agencies' accomplishments and planned activities to promote smart cards and the challenges to smart card adoption identified across the federal government. We also assessed available documentation and interviewed VA officials regarding their specific actions to

[1] GAO, *Electronic Government: Progress in Promoting Adoption of Smart Card Technology,* GAO-03-144 (Washington, D.C.: Jan. 3, 2003); *Electronic Government: Challenges to the Adoption of Smart Card Technology,* GAO-03-1108T (Washington, D.C.: Sept. 9, 2003); and *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology,* GAO-04-948 (Washington, D.C.: Sept. 8, 2004).

implement smart cards; however, we did not verify the information that VA provided in support of its initiatives. We performed our work in accordance with generally accepted government auditing standards during September and October 2004.

Results In Brief

The unique properties and capabilities of smart cards—plastic devices that use integrated circuit chips to store and process data—offer the potential to significantly improve the security of federal buildings, systems, data, and transactions. With the potential uses and associated benefits in mind, federal agencies, including the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and GSA have taken actions to advance the adoption of smart card technology governmentwide. In turn, numerous projects have been launched that offer many capabilities and tangible and intangible benefits. As of June 2004, 15 federal agencies had reported 34 ongoing smart card projects. Further, as understanding of smart card technology has increased, agencies have begun pursuing larger, integrated agencywide smart card systems aimed at better securing both physical access to facilities and logical access to computer systems and networks. Nonetheless, agency managers have faced considerable management and technical challenges in their efforts. These challenges have become less formidable, however, as management concerns about securing federal facilities and information systems have increased and as technical advances have improved the capabilities and reduced the cost of smart card systems.

The Department of Veterans Affairs is among a number of federal agencies currently pursuing large-scale, agencywide smart card initiatives. VA's Authentication and Authorization Infrastructure Project, begun in December 2002 and currently in a limited deployment phase, is planned to employ a combination of smart card and other technologies to achieve the capability to authenticate users with certainty and grant them access to information systems necessary to perform business functions. VA estimates that this project will cost about $162 million between 2004 and 2009, and enable it to issue 500,000 smart cards to its employees and contractors.

Background

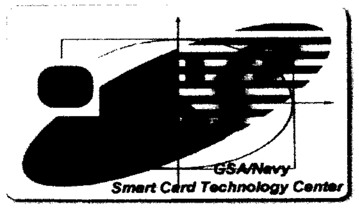
As you are aware, technology plays an important role in helping the federal government ensure the security of its many physical and information assets. Today, federal employees are issued a wide variety of identification (ID) cards that are used to access federal buildings and facilities, sometimes solely on the basis of visual inspection by security personnel. These cards often cannot be used for other important identification purposes—such as gaining access to an agency's computer systems—and many can be easily forged or stolen and altered to permit access by unauthorized individuals. In general, the ease with which traditional ID cards—including credit cards—can be forged has contributed to an increase in identity theft and related security and financial problems for both individuals and organizations.[2]

The unique advantage of smart cards—as opposed to cards with simpler technology, such as magnetic stripes or bar codes—is that smart cards can exchange data with other systems and process information rather than simply serving as static data repositories. Smart cards can readily be tailored to meet the varying needs of federal agencies or to accommodate previously installed systems. For example, other media, such as magnetic stripes, bar codes, and optical memory (laser-readable) stripes can be added to smart cards to support interactions with existing systems and services or to provide additional storage capacity. An agency that has been using magnetic stripe cards for access to certain facilities could migrate to smart cards that would work with both its existing magnetic stripe readers as well as new smart card readers. Of course, the functions provided by the card's magnetic stripe, which cannot process transactions, would be much more limited than those supported by

[2] See GAO, *Identity Theft: Available Data Indicate Growth in Prevalence and Cost,* GAO-02-424T (Washington, D.C.: Feb. 14, 2002).

the card's integrated circuit chip. Optical memory stripes (which are similar to the technology used in commercial compact discs) can be used to equip a card with a large memory capacity for storing more extensive data—such as color photos, multiple fingerprint images, or other digitized images—and for making that card and its stored data very difficult to counterfeit.[3] A typical example of a smart card is shown in figure 1.

Figure 1: A Typical Smart Card



Source: GSA.

Smart cards can be used to significantly enhance the security of an organization's computer systems by tightening controls over user access. A user wishing to log on to a computer system or network with controlled access must "prove" his or her identity to the system—a process called authentication. Many systems authenticate users by requiring them to enter secret passwords, which provide only modest security because the passwords can be easily compromised. Substantially better user authentication can be achieved by supplementing passwords with smart cards.[4]

[3] Cards with an optical memory stripe are known as laser cards or optical memory cards. For more information, see GAO, *Technology Assessment: Using Biometrics for Border Security,* GAO-03-174, (Washington, D.C.: Nov. 15, 2002).

[4] To gain access under this scenario, a user is prompted to insert a smart card into a reader to provide identifying information to the computer as well as type in a password. This authentication process is significantly more difficult to circumvent because an intruder would need to not only guess a user's password, but also to possess the same user's smart card.

Even stronger authentication can be achieved when smart cards are used in conjunction with biometrics.[5] Smart cards are one type of media that can be configured to store biometric information—such as fingerprints or iris scans—in electronic records that can be retrieved and compared with an individual's live biometric scan to verify that person's identity in a way that is difficult to circumvent. A system requiring users to present a smart card, enter a password, and verify a biometric scan provides what security experts call "three-factor" authentication, with the three factors being (1) something you possess (the smart card), (2) something you know (the password), and (3) something you are (the biometric). Systems with three-factor authentication are considered to provide a relatively high level of security.

Additionally, smart cards can be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. A PKI is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions.[6] A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) the parties will not be able to deny taking part in the transaction. Security experts generally agree that PKI technology is most effective when deployed in conjunction with smart cards.

Smart cards are grouped into two major classes: contact cards and "contactless" cards. Contact cards have gold-plated contacts that connect directly with the read/write heads of a smart card reader when the card is inserted into the device. Contactless cards contain

[5] For more information about biometrics, see GAO, *Information Security: Challenges in Using Biometrics*, GAO-03-1137T (Washington, D.C.: Sept. 9, 2003) and *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

[6] For more information about PKI technology, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

an embedded antenna and work when the card is waved within the magnetic field of a card reader or terminal. Contactless cards are better suited for environments where quick interaction between the card and reader is required, such as high-volume physical access. For example, the Washington Metropolitan Area Transit Authority has deployed an automated fare collection system using contactless smart cards as a way of speeding patrons' access to the Washington, D.C. subway system. Smart cards can be configured to include both contact and contactless capabilities; however, two separate interfaces are needed because standards for the technologies are very different.

Federal Agencies' Pursuit of Smart Card Technology Is Evolving and Involves Challenges

Since the 1990s, the federal government has considered the use of smart card technology as one option for electronically improving security over buildings and computer systems. In 1996, OMB tasked GSA with taking the lead in facilitating a coordinated interagency management approach for the adoption of multi-application smart cards across government. In this regard, GSA has taken important steps to promote federal smart card use. For example, since 1998, it has worked with several other federal agencies to promote broad adoption of smart cards for authentication throughout the federal government. Specifically, GSA worked with the Department of the Navy to establish a technology demonstration center to showcase smart card technology and applications and it established a smart card project managers' group and Government Smart Card Interagency Advisory Board.[7]

For many federal agencies, GSA's chief contribution toward promoting smart card adoption was its effort in 2000 to develop a standard contracting vehicle for use by federal agencies in procuring

[7] In 2000, GSA established the Government Smart Card Interagency Advisory Board to address government smart card issues, standards, and practices, as well as to help resolve interoperability problems among agencies.

commercial smart card products from vendors. Under the terms of the Smart Access Common ID Card contract, GSA, NIST, and the contract's awardees worked together to develop smart card interoperability guidelines—including an architectural model, interface definitions, and standard data elements—that were intended to guarantee that all the products made available through the contract would be capable of working together.

Further, OMB has begun taking action to develop a framework of policy guidance for governmentwide smart card adoption. Specifically, on July 3, 2003, OMB's Administrator for E-Government and Information Technology issued a memorandum detailing specific actions the administration was taking to streamline authentication and identity management in the federal government.[8] This included establishing the Federal Identity and Credentialing Committee to collect agency input on policy and requirements and coordinate the development of a comprehensive policy for credentialing federal employees.

Since 1998, multiple smart card projects have been launched in the federal government addressing an array of capabilities and providing many tangible and intangible benefits, including enhancing security over buildings and other facilities, safeguarding computer systems and data, and conducting financial and nonfinancial transactions more accurately and efficiently. As of June 2004, 15 federal agencies reported 34 ongoing smart card projects.

Initially, many of the smart card initiatives that were undertaken were small-scale demonstration projects that involved as few as 100 cardholders and intended to show the value of using smart cards for identification or to store cash value or other personal information. However, federal efforts toward the adoption of smart cards have continued to evolve as agencies have gained an increased understanding of the technology and its potential uses and benefits. Our most recent study of federal agencies' investments in smart card

[8] Office of Management and Budget, *Memorandum for Chief Information Officers of Departments and Agencies on Streamlining Authentication and Identity Management within the Federal Government* (Washington, D.C.: July 3, 2003).

technology, which we reported on last month,[9] noted that agencies are increasingly moving away from many of their earlier efforts—which frequently involved small-scale, limited-duration pilot projects—toward much larger, integrated, agencywide initiatives aimed at providing smart cards as identity credentials that agency employees can use to gain both physical access to facilities, such as buildings, and logical access to computer systems and networks.[10] In some cases, additional functions, such as asset management and stored value, are also being included.

To date, the largest smart card program to be implemented in the federal government is the Common Access Card program of the Department of Defense (DOD), which is intended to be used for identification by about 3.5 million military and civilian personnel. Results from this project have indicated that smart cards can offer many useful benefits, such as significantly reducing the processing time required for deploying military personnel, tracking immunization records of dependent children, and verifying the identity of individuals accessing buildings and computer systems.

Another large agencywide initiative is the Department of Homeland Security's (DHS) Identification and Credentialing project, an effort in which the agency plans to issue 250,000 cards to employees and contractors using PKI technology for logical access and proximity chips for physical access. Authentication is to rely on biometrics with a personal identification number as a backup. Further, GSA's Nationwide Identification is a recently initiated agencywide smart card project in which the agency plans to issue a single standard credential card for identification, building access, property management, and other applications to 61,000 federal employees, contractors, and tenant agencies.

While smart card technology offers benefits, launching smart card projects—whether large or small—has proved challenging to federal

[9] GAO-04-948.

[10] As of June 2004, agencies reported that more than half of the smart card projects previously identified as ongoing (28 of 52) had been discontinued because they were absorbed into other smart card projects or were deemed no longer feasible.

agencies and efforts to sustain successful adoption of the technology across government. Our prior work noted a number of management and technical challenges that agency managers have faced. These challenges include:

- **Sustaining executive-level commitment.** Maintaining executive-level commitment is essential to implementing smart card technology effectively. Without this support and clear direction, large-scale smart card initiatives may encounter organizational resistance and cost concerns that lead to delays and cancellations. DOD officials stated that having a formal mandate from the Deputy Secretary of Defense to implement a uniform, common access identification card across the department was essential to getting a project as large as the Common Access Card initiative launched and funded.[11]
- **Recognizing resource requirements**. Smart card implementation costs can be high, particularly if significant infrastructure modifications are required, or other technologies, such as biometrics and PKI, are being implemented in tandem with the cards. Key implementation activities that can be costly include managing contractors and card suppliers, developing systems and interfaces with existing personnel or credentialing systems, installing equipment and systems to distribute the cards, and training personnel to issue and use smart cards. As a result, agency officials have found that obtaining adequate resources is critical to implementing a major government smart card system.
- **Integrating physical and logical security practices across organizations.** The ability of smart card systems to address both physical and logical (information systems) security means that unprecedented levels of cooperation may be required among internal organizations that often had not previously collaborated, particularly physical security organizations and information technology organizations. In addition to the gap between physical and logical security organizations, the sheer number of separate and incompatible existing systems also adds to the challenge of establishing an integrated agencywide smart card system.

[11] Deputy Secretary of Defense, *Memorandum on Smart Card Adoption and Implementation* (Washington, D.C.: Nov. 10, 1999).

- **Achieving interoperability among smart card systems.** Interoperability is a key consideration in smart card deployment.[12] The value of a smart card is greatly enhanced if it can be used with multiple systems at different agencies, and GSA has reported that virtually all agencies agree that interoperability at some level is critical to widespread adoption of smart cards across the government. However, achieving interoperability has been difficult because smart card products and systems developed in the past have generally been incompatible in all but very rudimentary ways. With varying products available from many vendors, there has been no obvious choice for an interoperability standard. GSA considered the achievement of interoperability across card systems to be one of its main priorities in developing its Smart Access Common ID Card contract that I discussed earlier.
- **Maintaining security of smart card systems and privacy of personal information.** Although concerns about security are a key driver for the adoption of smart card technology in the federal government, the security of smart card systems themselves is not foolproof and must be addressed when agencies plan the implementation of a smart card system. Although smart card systems are generally much more difficult to attack than traditional ID cards and password-protected systems, they are not invulnerable. In order to obtain the improved security services that smart cards offer, care must be taken to ensure that the cards and their supporting systems do not pose unacceptable security risks. In addition, protecting the privacy of personal information is a growing concern and must be addressed with regard to the personal information contained on the smart cards. Once in place, smart card-based systems designed simply to control access to facilities and systems could also be used to track the day-to-day activities of individuals, thus potentially compromising the individual's privacy. Further, smart card-based systems could be used to aggregate sensitive information about individuals for purposes other than those prompting the initial collection of the information, which could compromise privacy. The Privacy Act of 1974[13] requires the

[12] Interoperability is the ability of two or more systems or components to exchange information and to use the information exchanged.

[13] 5 U.S.C. section 552a.

federal government to restrict the disclosure of personally identifiable records maintained by federal agencies while permitting individuals access to their own records and the right to seek amendment of agency records that are inaccurate, irrelevant, untimely, or incomplete. Further, the E-Government Act of 2002[14] requires agencies to conduct privacy impact assessments before developing or procuring information technology that collects, maintains, or disseminates personally identifiable information. Accordingly, agency officials need to assess and plan for appropriate privacy measures when implementing smart card-based systems and ensure that privacy impact assessments are conducted when required.

In considering these challenges, it is important to note that, while they served to slow the adoption of smart card technology in past years, they may be less difficult in the future because of increased management concerns about securing federal facilities and information systems and because technical advances have improved the capabilities and reduced the cost of smart card systems. Nonetheless, sustained diligence in responding to such challenges is essential in light of the growing emphasis on the use of smart card technology.

Recognizing the critical role that GSA, OMB, and NIST play in furthering the successful adoption of smart card technology, we made recommendations in January 2003 to these agencies that were aimed at advancing the adoption of smart card technology governmentwide. Specifically, we recommended that

- the Director, OMB, issue governmentwide policy guidance regarding adoption of smart cards for secure access to physical and logical assets;
- the Director, NIST, continue to improve and update the government smart card interoperability specification by addressing governmentwide standards for additional technologies—such as

[14] E-Government Act of 2002, P.L. 107-347, sec. 208 (Dec. 17, 2002).

contactless cards, biometrics, and optical stripe media—as well as integration with PKI; and

- the Administrator, GSA, improve the effectiveness of GSA's promotion of smart card technologies within the federal government by (1) developing an internal implementation strategy with specific goals and milestones to ensure that GSA's internal organizations support and implement smart card systems consistently; (2) updating its governmentwide implementation strategy and administrative guidance on implementing smart card systems to address current security priorities; (3) establishing guidelines for federal building security that address the role of smart card technology; and (4) developing a process for conducting ongoing evaluations of the implementation of smart card-based systems by federal agencies to ensure that lessons learned and best practices are shared across government.

As of last month, all three agencies had taken actions to address the recommendations made to them. Specifically, in response to our recommendations, OMB issued its July 3, 2003, memorandum to major departments and agencies directing them to coordinate and consolidate investments related to authentication and identity management, including the implementation of smart card technology.[15] NIST responded by improving and updating the government smart card interoperability specification to address additional technologies, including contactless cards and biometrics.[16] GSA responded to our recommendations by updating its "Smart Card Policy and Administrative Guidance" to better address security priorities, including minimum-security standards for federal facilities, computer systems, and data across the government.

However, three of our four recommendations to GSA remained outstanding. GSA officials stated that they were working to address

[15] OMB, *Memorandum for the Chief Information Officers of Departments and Agencies*, July 3, 2003.

[16] NIST, *Government Smart Card Interoperability Specification*, version 2.1, Interagency Report 6887 (July 2003).

the recommendations to develop an internal GSA smart card implementation strategy, develop a process for conducting evaluations of smart card implementations, and share lessons learned and best practices across government. The responsibility for one recommendation—establishing guidelines for federal building security that address the role of smart card technology—was transferred to DHS.

Recent federal direction contained in Homeland Security Presidential Directive 12[17] could further facilitate smart card adoption across the federal government. This directive, signed in late August, seeks to establish a common identification standard for federal employees and contractors to protect against a litany of threats, including terrorism and identity theft. The directive instructs the Departments of Commerce, State, Defense, Justice, and Homeland Security to work with OMB and the Office of Science and Technology Policy to institute the new standards and policies. With federal agencies' increasing pursuit of smart cards, directives from central management such as this one could be an important vehicle for ensuring that more comprehensive guidance is available to support and sustain the broader implementation of agencywide smart card initiatives.

VA Is Pursuing Agencywide Use of Smart Cards

Mr. Chairman, beyond the governmentwide assessment presented, you requested that we specifically address actions of the Department of Veterans Affairs in adopting smart card technology. Our report last month discussing agencies' investments in smart card technology identified VA as being among 9 federal agencies that currently have large-scale, agencywide smart card projects underway.[18]

[17] Homeland Security Presidential Directive 12/Hspd-12, August 27, 2004.

[18] GAO-04-948.

VA's effort—the Authentication and Authorization Infrastructure Project (AAIP)—was begun in December 2002 as an attempt to provide agencywide capability to authenticate users with certainty and grant them access to information systems necessary to perform business functions. The initiative, currently in a limited deployment phase, involves three core components: (1) a One-VA ID smart card; (2) an enterprise PKI solution;[19] and (3) an identity and access management infrastructure that addresses internal and external access requirements for VA users. VA currently estimates that, between fiscal years 2004 and 2009, this initiative will cost about $162 million.

The project is currently focusing on development of the One-VA ID card, which is to employ a combination of smart card and PKI technologies to store a user's credentials digitally.[20] According to project documentation, the One-VA ID card is intended to replace the several hundred methods for issuing identification cards that are currently in place across the department,[21] and improve physical and information security by strengthening the ability to authenticate users and grant access to information systems that employees and contractors rely on to perform VA's business functions.[22] As an official source of government identification credentialing, the card is expected to be compliant with Homeland Security Presidential Directive 12.

[19] VA plans to contract out a key component of the PKI known as a certification authority. For more information on contracting out certification authorities, see GAO-04-1023R.

[20] A PKI is a system of computers, software, and data that relies on certain cryptographic techniques for some aspects of security. A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction. For more information, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

[21] VA's facilities include 57 regional offices, 158 hospitals, 133 nursing homes, 7 centralized mail out pharmacies, and 9 regional loan centers.

[22] The One-VA ID card will not be issued to veterans or other VA beneficiaries.

VA is using a phased approach to develop and implement the One-VA ID card. This approach involves prototype testing followed by limited production testing at the department's facilities in the United States, and by 2006, the issuance of 500,000 cards with PKI credentials to its personnel. VA reported that it has already begun an initial limited deployment of the cards to about 15,000 to 25,000 users. The AAIP project manager anticipated that the results from this limited deployment would provide lessons learned for ensuring successful implementation, support, and training once full deployment of the One-VA ID card begins in early 2005. Further, the department has indicated that it plans to use information gathered from the limited deployment to create agency-wide policies and procedures for the full deployment of smart cards across all VA business units. As of late September, VA reported that fiscal year 2004 spending on the One-VA ID card totaled approximately $27 million for activities such as the acquisition of smart cards, card readers, and hardware support.

We have not yet had an opportunity to fully assess the outcomes of the department's One-VA ID card initiative or its actions to develop the enterprise PKI solution and identity and access management infrastructure that are also key components of this initiative. However, VA officials believe that the department is sufficiently positioned to successfully implement the smart card technology on an agencywide level. The AAIP project manager noted the chief information officer's involvement, as chair of the department's Enterprise Information Board, in monitoring progress of the project.

Further, as a participant in a number of governmentwide initiatives supporting the adoption of smart card technology, VA should be effectively positioned to carry out such an undertaking. Among its collaborations, VA is one of five agencies[23] using GSA's Smart Card Access Common ID contracting vehicle and plans to purchase smart cards for AAIP through the GSA contract. It is also a member of the Federal Identity Credentialing Committee, which provides guidance to federal agencies on the use of smart card technology that

[23] The other agencies are the National Aeronautics and Space Administration and the departments of Defense, Homeland Security, and Interior.

supports interoperable identity and authentication to enable an individual's identity to be verified within an agency and across the federal enterprise for both physical and logical networks. Collectively, the department's experiences and collaborations should lend strength to its own and overall federal efforts toward making smart cards a key means of securing critical information and assets.

In summary, the federal government is continuing to make progress in promoting and implementing smart card technology, which offers clear benefits for enhancing security over access to buildings and other facilities, as well as computer systems and networks. The adoption of such technology is continuing to evolve, with a number of large-scale, agencywide projects having been undertaken by federal agencies over the past several years. As agencies have sought greater use of smart cards, they have had to contend with a number of significant management and technical challenges, including sustaining executive-level commitment, recognizing resource requirements, integrating physical and logical security practices, achieving interoperability, and maintaining system security and privacy of personal information. These challenges become less difficult to address, however, as managers place greater emphasis on enhancing the security of federal facilities and information systems and technical advances improve the capabilities and reduce the costs of smart card systems. The challenges are also tempered as increased federal guidance brings direction to agencies' handlings of their smart card initiatives.

VA is among a number of agencies currently undertaking large-scale, agencywide projects to implement smart cards. While its project is still under development, VA has gained experience as a participant on governmentwide initiatives to further smart card adoption that should facilitate the increasing movement toward the use of smart cards as an essential means of securing critical information and assets.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the subcommittee may have.

Contacts and Acknowledgements

If you should have any questions about this testimony, please contact me at (202) 512-6240 or via e-mail at koontzl@gao.gov. Other major contributors to this testimony included Michael A. Alexander, John de Ferrari, Nancy Glover, Steven Law, Valerie C. Melvin, J. Michael Resser, and Eric L. Trout.

axalto

Testimony of Neville Pattinson
Director of Business Development, Technology and Government Affairs
Axalto, Inc.

Before the
Subcommittee on Oversight & Investigations
House Committee on Veterans' Affairs

October 6, 2004

Good morning, Mr. Chairman, Congresswoman Hooley and members of the subcommittee. Thank you for the opportunity and privilege to testify today at this hearing on Smart Card initiatives at the Department of Veterans' Affairs.

My name is Neville Pattinson and I am Director of Business Development, Technology and Government Affairs at Axalto (formally Schlumberger Smart Cards and Terminals prior to our IPO in May 2004). Axalto, which is based in Austin, Texas, is the largest supplier of Microprocessor Smart Cards. I have been directly involved with identity systems utilizing Smart Cards for over seven (7) years. In 2001, I was appointed as the Common Access Card Program Manager for Axalto and tasked to deliver the Department of Defense with their Java based Smart Cards (CAC). I led the effort that achieved the first ever FIPS 140-1 Level 2 certified Java Card along with achieving the demanding card body security and durability specification required by the Department of Defense. Axalto has now supplied over 5.5 million cards to the Department of Defense and several other government agencies via the GSA Smart Card prime contractors.

In addition to my position at Axalto, I am a Certified Information Systems Security Professional (CISSP); Chairman of the OpenCard Consortium; Board member of the International Biometric Industry Association (IBIA); an active member of the Smart Card Alliance and am an active member of the International Association of Privacy Professionals (IAPP). I am also honored to be representing a loose coalition of the three leading Smart Card manufacturers called the American Smart ID Card Alliance, which is a strong voice for security, privacy and efficiency of this technology in ID management.

Identity Management System Experience

Both Schlumberger and Axalto deployed identity systems throughout the company utilizing Smart ID Cards in order to secure our information, networks and facilities. We learned that implementing a corporate-wide identity system had several benefits. Our company realized that the information we managed – both ours and our customers' – was a valuable asset that required tight security and access control. Historically, our employees were required to maintain several username and passwords to access the many systems and facilities. Each independent system was enrolled separately and had its own administrator and community of users. Our employees ended up having to maintain multiple "identities" – which was not only cumbersome, but totally inefficient and ultimately not secure. By implementing an enterprise-wide Identity Management System, all employees' identities were managed centrally. Each of the legacy independent systems was then converted to use the Identity Management System as the only user authentication mechanism. By specifying standards across the enterprise – from physical access systems to desktop computing standards – we were able to migrate the company to an unprecedented level of global interoperability in less than two years. This allowed us to use the same corporate Smart ID Card badge for every level of employee. This system was based on similar technology to that deployed by the Department of Defense for authentication and access to any computer or facility in our multiple locations worldwide.

We have also seen a much higher degree of accountability as we use digital signatures on our e-mail to verify our content and maintain accuracy of the information. Secure communications are also possible when we use the encryption capabilities on top of digital signatures.

For example, when an employee terminates, the quick revocation of their credential becomes possible by informing the Identity Management System, which in turn disables access by that individual to all company resources – including building access control or logical access to computing or network services.

Identity Management Systems

Identity Management Systems are very beneficial when a centralized directory is maintained. An Identity Management System includes the:

- application to join the system by a user;
- enrollment of the individual;
- issuance of the credential and Smart ID Card; and
- management of the credential.

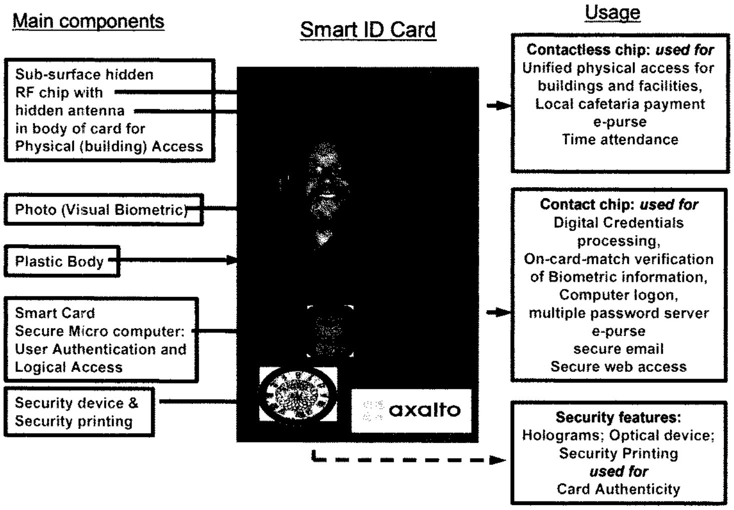
Without such a System in place, the security and interoperability of an enterprise is likely to suffer and add complexities and difficulty in securing all the issuance stations.

Physical access systems have traditionally been standalone implementations that cover a building, or a collection of buildings on a site. There is little connectivity of these systems over geographical distance or within corporations. It is also necessary to view physical access control as the responsibility of the local security officer, granting access rights to visitors from other locations by using their corporate identity and their Smart ID Card. However, the access rights to logical computing and network services should be done on an enterprise-wide scope ensuring a consistent and secure approach.

Smart ID Cards are a vital link in the chain of trust of an Identity Management System. They combine several security technologies into one convenient form factor. They are the local security agent of the issuer in the hands of the card-holder. Smart ID Cards consist of a physical badge in the shaped of a plastic card that incorporates several features such as visual security devices or printing, a tamper resistant Smart Card chip for logical access plus credential storage and optionally a second or possibly a third device for contactless RF physical access systems. Typically a photograph of the cardholder is printed onto the card along with other identifying information such as affiliation, expiry date, name, etc.

Figure 1 shows a typical Smart ID Card for visual, logical and Physical Access authentication & usage.

Figure 1. Smart ID Card Overview


Main components
Smart ID Card
Usage
Sub-surface hidden RF chip with hidden antenna in body of card for Physical (building) Access
Photo (Visual Biometric)
Plastic Body
Smart Card Secure Micro computer: User Authentication and Logical Access
Security device & Security printing
axalto
Contactless chip: used for Unified physical access for buildings and facilities, Local cafetaria payment e-purse Time attendance
Contact chip: used for Digital Credentials processing, On-card-match verification of Biometric information, Computer logon, multiple password server e-purse secure email Secure web access
Security features: Holograms; Optical device; Security Printing used for Card Authenticity

Benefits

Some additional benefits that have been seen after deploying Identity Management Systems are:

- Support desk cost reduction for resetting forgotten passwords;
- Increased physical access security and access control of employees;
- Decreased costs in operating multiple different physical access systems
- Highly secure access to IT infrastructure both locally and remotely via Smart ID Card enabled VPN connection; and
- High accountability, data integrity and confidentiality of users in system – for example, users can be certain of who sent an e-mail and also determine only specific users who are able to read the e-mail on arrival.

Other Benefits

- Smart ID Cards are privacy enhancing. The technology, when used in conjunction with defined best practices, will significantly augment an Identity Management System and protect the privacy of the users.
- An Identity Management System can assist organizations with HIPAA compliance, for example. Accountability of users, along with maintaining privacy of patient information, can be achieved with a comprehensive Identity Management System.
- Biometrics offer a strong mechanism for initially identifying a user (one-to-many matching) and subsequently verifying the user (one-to-one matching). When biometrics are combined with Smart ID cards they can support both types of verification. In Texas, to reduce fraud, a Medicaid pilot is using match-on-card fingerprint technology to authenticate the identity of individual as the receiver of the benefits.

Veterans' Affairs Identity Management System Implementation

We commend the Department of Veterans' Affairs for embarking on its own Identity Management System using Smart ID Cards for its employees. As there are already legacy physical access systems in place in several VA facilities, the project has embraced both a two and a three chip Smart ID Card. Both Smart ID Card variants are to contain a contact smart card chip for logical access and credential storage along with a second chip for new physical access systems as recommended by the IAB. One of the card variants will also contain a third chip for supporting the installed base of existing physical access systems based on RFID technology.

The Smart card project team within Veterans Affairs has spent considerable time performing feasibility studies and prototype evaluations in many areas to ensure the correct application of the technology to their systems and processes. This planning effort will lead to a better implementation as the project begins its rollout to the intended VA staff and contractor population. What they have learned will also benefit other agencies in their programs as all Federal agencies embrace the new HSPD-12 credentialing initiative.

Recommendations

It is important to define the scope of the Identity Management System along with specifying system-wide standards, specifications, privacy and security policies to ensure interoperability, consistency and proper usage. One should use standards and open specifications avoiding blind alleys or non-interoperability. It is important to define the criteria for enrollment, and the user authentication mechanisms once enrolled. A common data model is also important to ensure interoperability. Any project should first conduct a pilot, then revisit prior to commencing the enterprise-wide deployment. Once established, the Identity Management System will require maintenance and enhancements over time. I would recommend any program follow the well-proven: *"Plan, Do, Check and Act"* approach to implementation.

The usage of PINs along with Smart ID Cards is a good user authentication mechanism to determine user presence with the card. However, as biometrics become more established and the application determines the need to increase the authentication of the user, biometric authentication should be introduced where appropriate and cost effective as either a replacement or addition to the user's PIN.

Summary

Smart ID cards are a vital link in the chain of trust of any Identity Management System. The ability to master identity management within an enterprise or government agency brings tremendous savings, electronic communications security, user accountability, increased privacy and consolidated access control. Smart ID Cards are a convenient, proven, portable, cost-effective highly-secure technology for assisting with the management of identity. When combined with biometrics, the Smart ID Card offers a strong three-factor authentication of the card holder with: (1) Something they have (card); (2) Something they know (PIN); and (3) Something they are (biometric).

There is a wealth of experience within US Government agencies in deploying Smart ID Card-based Identity Management Systems. The Inter- Agency Board (IAB) and the Federal Identity Credentialing Committee (FICC) have also endorsed Smart ID Cards. The efforts to create the Government Smart Card – Interoperability Specification V2.1 by the National Institute of Standards and Technology (NIST) and the recent Homeland Security President Directive (HSPD-12) declaring an aggressive timeline for all federal agencies to implement a "Common Identification Standard" – makes it clear that interoperability is paramount for any government agency Identity System.

Thank you for the opportunity to testify before this distinguished subcommittee. I look forward to working with the members of the subcommittee in providing any help and guidance on this issue.

Statement

Of

Robert N. McFarland

Assistant Secretary for Information and Technology

Department of Veterans Affairs

Before the

Subcommittee on Oversight and Investigations

Committee on Veterans' Affairs

U.S. House of Representatives

October 6, 2004

Thank you, Mr. Chairman. I am very pleased to appear before this Committee representing the Secretary and the Department's information technology programs. On March 17, 2004, I appeared before this Committee and gave you an overview of VA's information technology processes and projects. I am here today to provide you with an update regarding VA's Authentication and Authorization Infrastructure Project (AAIP). We currently have the Department positioned almost 12 months ahead of the mandates contained in Homeland Security Presidential Directive12 (HSPD-12), titled "Policy for a Common Identification Standard for Federal Employees and Contractors." VA has achieved this position, which is well ahead of many agencies, because we have continuously synchronized AAIP with government deliberations and involvement in the process that lead up to HPSD-12. We view this as a success story. Events continue to validate the merits of the AAIP approach taken by VA, and the Department continues to display substantial leadership in the Federal arena.

Currently, VA has a Federal Manager's Financial Integrity Act (FMFIA) "material weakness" related to account management. AAIP plays a significant part in addressing this issue by creating better account management controls, two factor authentication with smart cards, and a reduction on the reliance of static passwords. The VA's Office of Inspector General (OIG) has reviewed AAIP, and believes that it is a significant move toward removing this outstanding concern.

AAIP specifically considers, and sets up strategies to effectively comply with, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security

Rule, the Gramm Leach Bliley Act for financial services, the E-Government Act of 2002, including the Federal Information Security Management Act (FISMA) provisions, and OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, as well as the OMB memo entitled Streamlining Authentication and Identity Management within the Federal Government. As such, AAIP will make a significant, cost-effective contribution to VA's commitment to achieve regulatory compliance.

The benefits of AAIP were apparent in preliminary tests with the Drug Enforcement Agency (DEA), wherein AAIP demonstrated the ability to save up to 45 minutes in processing time associated with pharmacy transactions. This can be achieved through the application of digital signature, which complies with DEA regulations, reduces paperwork, and substantially reduces unintended errors. In the process, service to the veteran is greatly enhanced in a cost effective manner.

During detailed testing of smart card usage in a "thin client" environment, AAIP demonstrated the ability to recover up to 45 minutes per day of clinician time through simplified logon processes. VHA has tens of thousands of clinicians on duty at any given period of a day, and any recovery of productivity of this magnitude will create significant efficiencies, cost savings, and result in better patient care for our veterans.

AAIP is directly aligned with the Department's E-Sign initiative. Starting in FY 2005, E-Sign oversight has been transferred under the purview of AAIP. As AAIP implements E-Sign technology, VA will make significant improvements in the use of E-Sign technologies that will streamline veteran services and reduce processing costs incurred by VA. As a net result, this should be dramatically reflected in VA's Government Paperwork Elimination Act and Government Performance and Results Act reporting.

VA currently has several hundred thousand users of computer systems, many with their own separate accounts and passwords. This creates a tremendous account and password burden on VA to operate systems day-to-day. Through AAIP's use of smart cards, VA is setting a progressive architecture and strategy that will improve password management. Smart cards do not require 90 day password rotation, and we have established criteria to implement single sign on (SSO) technologies, minimizing the number of passwords the users have to remember, while leveraging the inherent security of smart cards.

AAIP conducted a detailed analysis of physical access control systems, as they apply to the use of a smart card that is enabled for building access control. Findings indicate that VA could achieve several million dollars in annual cost avoidance through a more efficient strategy related to physical access control system operations.

During FY 2004, the AAIP staff negotiated an enterprise site license with ActivCard for smart card middleware and management software for $12 million, structured into a 4 year lease. The street price of the software is projected at $52 million, resulting in a significant savings.

Internally, VA's Office of the Inspector General (OIG) has identified that AAIP will make a significant contribution towards addressing the finding of "material weakness" and the program will be central to addressing HIPAA security considerations. In addition, this project has been briefed to the national Labor Unions for VA, and has been received favorably. The Labor Unions believe that the employees should have an official ID card and that other derived benefits improve the efficiency of VA.

Externally, over the past 12 months, the Government Accountability Office (GAO) has consistently communicated positive findings related to AAIP and the smart card program. GAO suggested that VA speed up the deployment process from the original 42 month deployment period. VA now has an 18 month deployment period identified in the project planning documents.

AAIP is currently conducting a pilot with the E-Authentication E-Government Initiative, managed by the General Services Administration (GSA), which will test the use of smart cards and public key infrastructure (PKI) credentials against agency systems. This project directly supports the President's Management Agenda, and VA is pleased to act as a leader in this area of government.

VA staff assumed leadership over the Shared Service Provider (SSP) Subcommittee of the Federal Identity Credential Committee (or FICC), acting as the Chair. Starting in September 2003, through the collaborative efforts of the National Institute of Standards and Technology (NIST) and other agencies, the SSP Subcommittee established the evaluation criteria to successfully publish a listing of qualified managed PKI service providers that are available to all federal agencies. As a result, the Federal Government now has a core list of authorized PKI managed services providers, directly supporting the Federal Identity Credentialing Committee chartered by OMB in July 2003.

In September 2004, VA became one of the first Federal agencies to issue a contract to a federally approved managed PKI service provider under the FICC's SSP program. This activity is directly in line with the vision and spirit of OMB's memorandum entitled "Streamlining Authentication and Identity Management within the Federal Government," dated July 2003.

Various Federal agencies are now approaching VA for assistance and access to documentation, processes, and procedures employed by the project to date. This includes the Department of Defense, Department of Interior, National Aeronautics and Space Administration, and the Department of Transportation. The range of requests spans from access to requirements documents, to program structure and testing methodology. While VA recognizes that other agencies have lessons learned that we can benefit from, we are proud of our successes in this area and our ability to share our experience with other agencies.

From a program management perspective, AAIP is directly aligned with mandates from OMB, the Federal CIO Council, the Federal Identity Credentialing Committee and internal VA publications such as the VA Strategic Plan, the VA's Information Technology Strategic Plan, and the VA Enterprise Architecture documents.

The AAIP staff formulated a detailed, structure prototype process to evaluate the injection of smart cards and PKI into the VA enterprise. The prototype process included eight specific areas: remote access, network access, wireless access, thin client access, web access, database access, legacy access and physical access. The prototypes allowed VA to identify what would work, what would not work, and what changes could be made to achieve functionality.

VA is currently participating in the government smart card aggregate buy of smart cards. Initially, VA will procure approximately 100,000 smart cards based on the new Government Smart Card Interoperability Specification v2.1 (GSC-IS). This procurement is being managed by the General Services Administration, pursuant to guidance from OMB. VA will start to receive these smart cards as early as October 2004. Part of the order includes new generation dual-physical antenna cards. These cards, at select facilities, will support co-existence with the current physical access control systems and the ability to migrate to physical access control systems that are compliant with the new GSC-IS specifications.

During the prototype phase of AAIP, the project established a best practices systems engineering approach where the technology was first tested in a controlled lab environment, and then field tested at VA facilities. Examples include successful testing of AAIP and smart card usage for remote access over the enterprise gateways, integrated smart card logon at approximately 10 separate locations across VA, secure testing of smart card logon with wireless technologies, web access, database, and certain legacy devices. The staff also established evaluation processes for physical access control systems, and now serves as the central resources across VA as facilities plan efforts to move to the new federal GSC-IS standards, based on International Organization for Standardization 14443.

Finally, I believe VA has made great progress regarding this important effort, positioning ourselves to implement a smart card program ahead of the schedule outlined in HSPD 12. I remain committed to implementing a smart card program that provides improved business functionality, increased security, and enhanced service to our nation's veterans.

This concludes my written statement. Thank you, Mr. Chairman, for the opportunity to discuss these important matters. I will be happy to answer any questions you might have.

Not for publication until released by the Subcommittee

Prepared Statement of
Robert J. Brandewie
Director, Defense Manpower Data Center

Before the House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations

Oversight Hearing on "The Status of the Department of Veterans' Affairs Smart Card Initiative(s)"

October 6, 2004

Good morning ladies and gentleman. As the Director of the Defense Manpower Data Center (DMDC), I am responsible for the development, fielding, and maintenance of a number of Department of Defense (DoD)-wide systems. Today, I will discuss the DoD smart card initiative known as the Common Access Card, commonly referred to as the CAC. In addition, I will address DoD's efforts with the National Institute of Standards and Technology (NIST) to facilitate the fulfillment of the requirements directed in the Homeland Security Presidential Directive 12 (HPSD-12).

DoD recognized the importance of strengthening the identification and authentication process in the mid 1990's, given the increasing ease with which credentials could be counterfeited or fraudulently obtained. Also, the Department recognized the increasing importance of network based communication, and the rise in the attractiveness of e-business and e-government transactions for efficiency and cost effectiveness. The response in both cases was to strengthen the business process for the identification and credentialing of our military members, civilian employees, and family members. The Department began work in November of 1999 to modify the DoD Identification Card from a relatively low technology card to a smart card with an integrated circuit chip (ICC). The new smart card would be an authentication token for the military member or employee, and also, contain Public Key Infrastructure (PKI) cryptographic keys and certificates. The Department made a conscious decision to use the smart card as an authentication device instead of a data storage device for three reasons: (1) minimize the problem of synchronizing the card and the database, (2) minimize the concern of always chasing a larger capacity card, and (3) most importantly, mitigate any risk for our military members were they to be captured in time of hostilities.

Such a card was critical to the secure use of the network capabilities, and therefore, would increase security while at the same time enabling more efficient and effective web-based transactions for a variety of DoD business processes. The initial test cards were produced in December of 2000 and full production of this new card, called the CAC, began in September of 2001. By July of 2003, the full infrastructure was rolled out to 945 sites in 27 countries and the program was fully implemented. Today, more than 5.5 million CACs have been issued at the rate of more than 10,000 per day. Currently, about 3.2 million DoD active and reserve military members, civilian employees and DoD contractors carry a valid CAC. This includes the 1.75 million Army, Navy, Air Force, and Marine Corps active duty and Selected Reserve members in the DoD; the 49,500 Coast Guard members in the Department of Homeland Security (DHS); the 6,000 Public Health Service (PHS) members in the Department of Health and Human Services (HHS); and the 250 National Oceanographic and Atmospheric Administration (NOAA) members in the Department of Commerce (DOC).

At the same time, and just as importantly, DoD has focused its Personnel Identity Protection program on the business process; securely identity proofing and vetting individuals and binding their identity to a credential, the CAC, at issuance. The process of performing secure, upfront identity proofing and vetting is the foundation upon which a sound credentialing infrastructure is built. To do less weakens the resulting credential, as well as the trust that can be placed in the credential.

The first step in the Personnel Identity Protection process is strong authentication of the individual. This requires a business process that provides sufficient evidence of identity and a face-to-face interaction between the individual and a trusted agent.

Providing sufficient evidence of identity should include, at a minimum, checks of public records, background investigations, and examination of primary documents to name a few. The second step in the process is to bind that confirmed identity to a management system. A credential is the best linkage to a Personnel Identity Protection system. Binding the credential to the individual is the third step in the process. The use of biometrics and Personal Identification Numbers (PINs) are good mechanisms to bind the credential to the person, and both are used in the DoD program. This step fixes the individual's identity to the credential from that point forward. The credential then becomes an identity proxy and a token for providing logical and/or physical access. Step four is the authentication of the credential at all physical and logical access points. Step five is revoking the credential, as close to real-time as possible, when the individual's affiliation is terminated or when the credential is lost, stolen, or compromised (similar to what happens in the credit card industry). The last step in the Personnel Identity Protection system is to safeguard personal identity information from unwarranted disclosure. In an age where identity theft is the fastest growing white collar crime, this last step is critically important.

There are characteristics of the Department's issuance process that contribute to its strength and mitigate the vulnerabilities of any credentialing system. First, the credentialing system is linked to a central repository of affiliated people entitled to the Department's credential. This repository is fed by approximately 75 authoritative sources of military member and civilian personnel information in the DoD. This authoritative source of identity and affiliation information is the Defense Eligibility Enrollment Reporting System (DEERS). Second, the issuers of credentials are vetted before they are given access to the system by the Defense Security Service (DSS). Third, the issuers of credentials are authenticated using their CACs (requiring a PIN), their biometric (a fingerprint), and the workstation being used. Likewise, the cards that they are issuing are authenticated against a card management system and a logistics portal. All of these factors must pass security scrutiny and be authenticated and approved before a card is issued. Fourth, the issuers of credentials are not able to add new people to the repository because their eligibility for a DoD credential must be independently verified by an authoritative data source. Finally, the issuers of credentials do not grant privileges.

The CAC is used for authentication of identity, logical access to DoD networks and systems, and for physical access to DoD buildings and facilities, the latter being the application that is the slower of the three to be implemented. Reforms in electronic business (to include paperless contracting, wide-area workflow, and other procurement and finance applications), travel re-engineering, and expanded use of the government-wide commercial purchase card program coupled with information assurance for data and identity authentication have presented new opportunities to use smart card technology as an enabling tool for enhancing business processes. The CAC is used for various business applications such as a replacement for passwords, food service, deployment/warrior readiness, and manifesting. DMDC continues to work with the Components and other Defense Agencies to develop specific applications to enhance military readiness and improve the quality of life.

As the use of the CAC for applications expands and the technology becomes more advanced, additional space on the card is required. In March of 2005, DoD will move to a 64K contact card to meet emerging requirements and to be compliant with the

Government Smart Card Interoperability Specification (GSC-IS) v2.1. In response to requests from the physical access community, DoD anticipates piloting contactless smart card technology by end of Summer/Fall 2005. DoD is also working towards an enterprise biometrics solution for an additional layer of security on the card. The Department has been capturing digital fingerprints on military personnel for approximately four years and has prints on almost all uniformed members in its central repository. As part of CAC issuance, DoD captures two fingerprints on military, civilian and contractor personnel, if we do not already have them. At re-issuance, the system performs a fingerprint check between the live person and the database to ensure it is the same person. In the event of a non-match, which can occur for a number of reasons, the operator is required to take additional steps to verify identity before issuing a card. DoD is changing its business processes to have digital fingerprints captured at enlistment processing stations for the purpose of background checks by the Federal Bureau of Investigation (FBI). The fingerprints would also be sent to the central repository used in the credential issuance process. This permits the Department to ensure that the person processed for enlistment is the same individual showing up at basic training, further strengthening the Personnel Identity Protection process. While considerable investigation of the utility of other biometric measures is ongoing in the DoD, under the auspices of the DoD Biometrics Management Office (BMO), current plans for the CAC are limited to fingerprints. To introduce a new card (64K) or other technology change (contactless) into the system, a little over three years is required to implement and replace all active cards. To change data or applets (e.g., biometrics) stored on the card, much less time is required since it is possible to securely change certain software on the card using post issuance capabilities.

DMDC maintains the identification information known as the Defense Enrollment Eligibility Reporting System (DEERS), for generating Uniformed Service sponsor and family member benefits, entitlements, and identification credentials. The Real-time Automated Personnel Identification System (RAPIDS) is used to issue the credential of affiliation with DoD, and it relies on the information stored in DEERS. The CAC serves as the assertion of identity and is authenticated against the DEERS database, global directory services, or DoD PKI services in real-time whenever possible. The granting of logical and physical access privileges remains a local policy and a business operation function of the local facility, but must function in concert with Personnel Identity Protection policies and procedures.

There is not an easy solution to the worldwide problem of knowing, with absolute certainty, exactly who each person is. Many organizations tend to focus on the latest technology such as smart card technology, PKIs, biometrics, and sophisticated physical and logical access control systems. The technology is important; however, the risks are large, and it is not enough when protecting the identity and privacy of individuals. Through the use of a strong and rigorous issuance process, followed by strong electronic authentication of the credential whenever it is used, it is far more difficult for someone to steal another individual's identity. The Defense Biometrics Identification System (DBIDS), Defense Cross-Credentialing Identification System (DCCIS), and Defense National Visitors System (DNVS) meet the objective of the Personnel Identity Protection program.

DBIDS is a theater, or regional based force protection system developed initially by DMDC at the request of United States (US) Forces Korea. In brief, it uses cards, photographs, and fingerprints to control access to all gates to US facilities on the Korean peninsula. All personnel having access are required to go through a registration process where biometrics are captured and cards are issued to those who do not already have either a CAC or some other DoD issued credential. A "one-to-many" fingerprint check is made to identify anyone already in the database. A server based database, downloaded to the gates, is available throughout Korea, and is designed to operate in the absence of communications, if necessary. Gate guards have wireless handheld devices capable of scanning a card and determining whether it is genuine and valid. The devices bring up a photograph of the person from the database, and perform a fingerprint check in a matter of seconds. Any or all of these checks can be done depending on the threat conditions. The system also notifies guards if someone should be barred or even arrested. Subsequently, this system was fielded in Europe and Kuwait. Plans are underway for fielding this system in Japan, Qatar, and Forts Hood and Polk.

The Defense Cross-Credentialing Identification System (DCCIS) is an initial proof-of-concept for testing a standards-based (X.509) implementation of existing PKIs, and potentially, other commercial identity schemas. This proof-of-concept proposes to resolve the interoperability difficulties between DoD and its commercial partners. DCCIS would be used in instances where there is a reciprocal requirement for enrolling and identifying personnel and granting them various access privileges to both physical sites and logical networks, but where there is also a requirement to maintain control and access of an organization's own data. DCCIS enables participating DoD facilities to achieve strong and interoperable identity verification and authentication of participating contractor/private sector personnel who present a company-issued trusted credential. This system provides a means to share identity authentication information across organizational network infrastructure boundaries. The ultimate goal is to create a "federated" system between the DoD and its industry partners that reflects the interests of each party in retaining control of its own policies; including the access control policies at the local level.

The Defense National Visitors System (DNVS) enables participating DoD facilities to perform physical authentication procedures on DoD personnel presenting CACs for entrance into DoD facilities. It is a web-based system that verifies physical access credentials with a sub-second response time. In addition, DNVS can be DCCIS enabled. In this case, a participating DNVS facility would connect with DCCIS member organization databases in order to authenticate visiting personnel from those organizations.

I would like to conclude my statement with a few remarks about the importance of using standards-based commercial products whenever possible. The ability to write specifications in terms of well-defined and accepted national and international standards, and to have laboratories that can test products and certify that these standards have been met, ultimately reduces the cost to the users and promotes interoperability between and among Federal agencies, industry, business partners, and other countries. There has been a concerted effort to use such standards in the development and implementation of the CAC. The General Services Administration (GSA) and the National Institute of Standards and Technologies (NIST) have been critical partners in this process. As a result, it is very easy for other organizations to adopt all or part of what DoD has done with the CAC. DoD has worked and will continue to work with other Federal agencies wanting assistance with similar programs, or to provide information on valuable lessons learned. For example, DoD and the Department of Veterans' Affairs (VA) have been in contact to share technical approaches to credentialing over the past two years. There have been discussions of DoD hosting VA infrastructure as well as the transfer of VA expertise in using credentials in the medical business space to DoD. Additional conceptual discussions of the DoD issuing a VA credential to departing DoD members promises cost savings, in addition to strengthening the transfer of a member's identity from organization to organization. These concepts can reduce costs as well as provide better service to our common beneficiaries.

Thank you for the opportunity to address the Subcommittee.

WRITTEN COMMITTEE QUESTIONS AND THEIR RESPONSES

Hearing Date: October 6, 2004
Committee: House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Member: Representative Buyer
Witness: Robert J. Brandewie
Question # 1

Question: What security standards are in place at the Department of Defense for lower level employees?

Answer: All employees of the Department of Defense (DoD) receive vetting before or coincident with employment. All military members receive entrance national agency checks and local agency checks; all DoD civilians receive a suitability check that includes a national agency check. Contractors are not as easy to characterize as they perform many different functions. However, the intent of the DoD policy on the Common Access Card (CAC) is to issue these cards only to those contractors who require logical access to DoD information systems. The Department has implemented a series of security standards for individuals who have access to DoD computer systems. These standards are detailed in DoD 5200.2-R, "Personnel Security Program." Security regulations and procedures are defined for vetting personnel in three categories of access. Minimum requirements for any Automatic Data Processing (ADP) clearance include a successful national agency check. Therefore the three categories of employees who are Common Access Card holders have met these minimum DoD security requirements and many, including those holding security clearances, have been much more extensively vetted.

With respect to those employees and military members who issue the Common Access Card, the Department of Defense uses operators, called verifying officials, who work for the Military Services. DoD regulations require a successful national agency check for all military, DoD civil servants and contractors who serve as verifying officials for the Real-time Automated Personnel Identification System (RAPIDS). In addition, US Citizenship is required for all verifying officials issuing CAC/Public Key Infrastructure (PKI) certificates. The Defense Manpower Data Center (DMDC), the organization responsible for the operation of RAPIDS, provides the guidance to the Services for the vetting of verifying officials. A Security Checklist requiring that every RAPIDS Site Security Manager sign and confirm compliance to the vetting and US citizenship requirements is under development and will be implemented in the very near future. Web-based training, to include a security module with vetting requirements, is also being developed. Periodic/yearly certification will be required for all verifying officials prior to gaining access to RAPIDS. Certification will result from successful completion of a web-based test on all training modules.

Hearing Date: October 6, 2004
Committee: House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Member: Representative Buyer
Witness: Robert J. Brandewie
Question # 2

Question: On page 11 of your testimony, you stated that DoD and VA have been in contact to share technical approaches to credentialing over the last 2 years? Could you elaborate on what this means?

Answer: Development of secure smart card based credentialing system is a complex and potentially expensive undertaking. The issues that must be addressed cover both technical issues of card architecture and management to business process issues of identity proofing techniques. The Department of Defense (DoD) began its current Common Access Card program in 1999 and has had to address the range of issues. Discussions with the Department of Veterans Affairs (DVA) began before DoD had issued production cards as DVA tried to assess the applicability of a secure credential to DVA business processes. The DVA Chief Information Officer visited the Defense Manpower Data Center (DMDC) to learn more and to decide whether to include a secure smart card based credential program in the DVA enterprise plan. Ultimately, the decision was made to do that and the two agencies have met over the course of the past two years and shared technology and approaches to credentialing of employees. Discussions have ranged from DoD taking on the task of issuing DVA cards to DoD providing expertise and assistance. The result of those efforts is that the DVA is preparing to issue cards that share DoD's technology, methodology, and implements common software modules between the two Departments. This means that much of the issuance technology that was developed to support DoD will be incorporated in the DVA implementation and also that the cards will share a common card architecture and some common software. This makes interoperability between the two Departments much easier from a technical viewpoint.

There have been additional discussions concerning changing business processes to allow DoD to issue a 'Veteran's Card' for the DVA when DoD personnel leave the military. This could mean that the DoD infrastructure would provide the veteran with a VA card as he leaves DoD. This concept would be advantageous to both Departments as well as the veteran. Additionally, DoD is developing a resource estimate to provide backup for their credential management system. Both of these discussions are proposals that both parties have discussed but have not progressed beyond that point.

Hearing Date: October 6, 2004
Committee: House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
Member: Representative Buyer
Witness: Robert J. Brandewie
Question # 3

Question: What safeguards are in place to prevent card abuse at minimum level security?

Answer: The Common Access Card (CAC) has both physical and logical features which prevent it from being easily counterfeited or misused. On the physical side, the CAC is a complex card composed of seven separate layers of plastic composites. This makes it more durable and increases its longevity. The CAC printing process uses a dye sublimation which imbeds the ink colors into the plastic material of the card. This year we are moving to reverse transfer which actually places the ink on a clear sheet which is laminated to the card. This is a more secure mechanism because if the clear plastic were removed from the card the tampering would destroy the card. This is the same process that the State Department now uses for production of the US passport. There is also an Optical Variable Device (OVD) embedded as one of the card layers. It contains an image which changes color as the card is tilted in the light. On the back side of the card there is a picture of the individual called a ghost image. This image is actually etched into the card, so if the picture on the front was 'changed' someone could also check the back of the card to see if it matched the front side. In the next several years, the CAC program will introduce other topographic anti-counterfeiting safeguards in order to constantly 'evolve' the card surface to prevent easy card duplication.

On the logical side, there is a Personal Identification Number (PIN) which is known only to the cardholder. When entered properly, the PIN opens the card to PIN protected services. The cardholder has three attempts to enter the PIN correctly. After the third attempt, the card is locked and no longer available for use. The cardholder must return to a registration site, either RAPIDS or a Service sponsored CAC PIN Reset (CPR) machine, to unlock the card. The PIN reset service must be done with a verifying official, who corroborates the card and the cardholder are visually the same. Additionally, the application validates the fingerprint of the cardholder and displays the photograph stored on the card to the verifying official, before allowing the PIN to be reset.

Another safeguard to card abuse is that DMDC, as the card issuer, controls all write privileges to the card. This translates to a set of master keys which the card issuer controls and which are diversified for each individual card in the system. Only the card issuer master keys can 'possess' the card by matching the diversified key which is stored on the card. So only the card issuer can personalize the card with person and personnel data.

Questions for the Record
From Chairman Steve Buyer
Subcommittee on Oversight and Investigations
Committee on Veterans Affairs
October 6, 2004

Hearing on VA' Smart Card Initiative(s)

Question 1: How many VA smart card projects or demonstrations have been initiated in the last 10 years? How much money has been spent on each of these projects and demonstrations? How many of them have been implemented and are still in existence?

Response: Two VA smart card projects or demonstrations have been initiated in the last 10 years:

a. The Authentication and Authorization Infrastructure Project (AAIP) is an OMB approved project with a 5 year budget of $172 million. The project provides for the One-VA ID card based on a smart card form factor, and is compliant with the mandates of HSPD-12, issued by the White House on August 27, 2004. In FY04, the project expended approximately $26 million. Most of these funds were targeted at infrastructure, systems, issuance stations, and smart card stock along with technical support costs.

b. The One-VA Express Card pilot ran from January to May 2001. This pilot involved two locations, Iron Mountain, MI and Milwaukee, WI. The purpose was to determine if the best and most cost effective technology to make registration and clinical data available between medical facilities in real time was to use a) the smart card or b) a network centric technology available through VistA. Expenditures for the pilot were $5.3 million. Approximately 40,000 cards were issued. This pilot was not implemented nationwide because the network-centric approach using VistA was preferred and found to be more cost effective.

In addition, VA has in place two other card projects, neither of which contains a computer chip:

a. The Veterans Identification Card (VIC) Replacement Project replaces existing veteran identification cards that display sensitive veteran information and utilizes aging hardware that is failing and can not be repaired.. The primary purpose of project was to remove visible personal identifying information (such as SSN and date of birth) from face of cards to protect veterans from identity theft. The photo of veteran was enhanced from black and white to larger color image. The VIC Project was a result of the halt of the One-VA Express Card project. To the extent possible, the VIC project re-used One-VA Express Card software developed for the project and learned from the work done during the pilot.

VIC is a "dumb" card, not a smart card. VIC is able to reuse existing software for the workstation application, VistA, and the National Card Management Directory from the One-VA Express project with some modifications. National deployment began August 30, 2004 and will be completed in November 2004. Estimated total volume of cards produced is 2.5 million in the first year of production and 1 million in subsequent years. First year production budget is $3.5 million that includes funding for 2 workstations and camera configuration for each medical center and the external card vendor production costs for the 2.5 million cards. Funding in subsequent years will be covered by the Health Eligibility Center budget.

b. The Miami VA Medical Center swipe card pilot was started in August 2003 and is currently being conducted. This pilot was designed to validate the use of one specific technical solution in an effort to collect data on physician acceptance of an automated timekeeping system, obtain feedback from physicians on the use of the technology, and to provide guidance concerning timekeeping processes for part-time physicians. Already planned expenditures for the system of readers and cards were expedited so no additional, unbudgeted funds were used. Staffs involved in coordinating the pilot have done this as a collateral duty. No additional staff or contractors were hired to support the effort. Approximately 60 cards issued. The technology was evaluated and found to function successfully at providing data on physician entrance and exit. It also is compatible with AAIP technology.

Question 2: Under what circumstances would a VA employee be required to provide fingerprint and/or iris scan identification?

Response: Currently the only biometric captured is a digital photo, which is accomplished to comply with the requirements of the Common Certificate Policy (www.cio.gov/ficc). This is the same digital photo that is printed onto the cards. Unless emerging federal policy (FIPS-201) requires otherwise, VA does not plan to collect fingerprint and/or iris scan templates.

Question 3: Who makes the determination about the issuance of a smart card?

Response: Smart card issuance is only authorized when an appropriate, designated management official requests that a credential be issued.

Question 4: How many smart card projects are currently underway? Where do these projects reside? Are they all within the IT department?

Response: One smart card project is currently underway and that is the AAIP Project managed by the Office of Cyber and Information Security, Office of the Assistant Secretary for Information and Technology.

Question 5: How much money has VA spent on its smart card projects in the last 10 years?

Response: VA has spend $35.3M on smart card projects in the last 10 years; .AAIP - $30M from FY03 – FY 04; and One-VA Express Card Pilot - $5.3M from 01 FY 01 – 05 FY 01.

Question 6: Why did it take three years to address and implement additional safeguards after a $6 million compensation and pension fraud case was uncovered at the Bay Pines, Florida Regional Office?

Response: Following discovery of the fraud case, the Under Secretary for Benefits (USB) requested the Office of Inspector General's assistance in identifying internal control weaknesses that might facilitate or contribute to fraud in the compensation and pension (C&P) benefits program.

The OIG audited internal controls for adjudication and payment of C&P benefits at the St. Petersburg Regional Office. The July 2000 OIG audit report made 15 recommendations with 26 independent reportable action items to strengthen internal controls. The recommendations generally addressed areas such as physical and electronic security of sensitive files and records; access and security controls for VBA's benefit payment system, the Benefits Delivery Network (BDN); and employee conflict of interest.

VBA took prompt action to strengthen procedural controls for the adjudication of claims of former employees, relatives, and veteran service organization (VSO) employees. Action was taken to ensure VBA and VSO employee claims folders were transferred to the VARO of jurisdiction and properly secured. VARO directors are required to certify this process annually. Certification is also required annually to ensure that all employee relatives have been identified and records of family members have been appropriately transferred and electronically secured.

The Under Secretary for Benefits advised all employees about the expectations of employee conduct and avoidance of conflict of interest and instituted an annual all-employee ethics training program.

VA also took action on the OIG's recommendations to strengthen the system audits and controls of the BDN. However, a number of the recommended changes to the BDN were determined to be infeasible because of the antiquated architecture of this complex system and the resource levels that would be required to make the recommended changes. VA therefore put new interim controls in place and committed to making the recommended changes in the Modern Award Processing System, a major component of the BDN replacement system known as VETSNET.

The OIG's recommendation from the St. Petersburg audit that VBA establish a system control to prevent release of payments greater than $15,000 without the authorization of a third person was among those determined to be infeasible because of the antiquated BDN system architecture. However, following discovery of the Atlanta case, VBA took additional steps to strengthen the integrity of the compensation and pension program by immediately instituting a mandatory large payment verification process. Effective in September 2001, regional office directors are responsible for verifying and certifying the propriety of all retroactive payments of $25,000 or more. Since the start of this review, nearly 58,000 payments totaling over $2.8 billon have been reviewed through this process. The process is audited by the OIG through their Combined Assessment Program Reviews and VBA C&P Service site visits. The system-generated third-person authorization process as recommended by the OIG is included in the design of the VETSNET Modern Award Processing System.

Of the 26 internal control action items recommended by the OIG following the audit of the St. Petersburg Regional Office, 21 have been fully implemented and are considered closed by the OIG. Of the remaining five action items, two are awaiting OIG's validation of VBA's report that they have been fully implemented. A third action item is expected to be closed by the OIG by the end of calendar year 2004. The remaining two action items recommend system controls to restrict adjudication of employee claims to only the regional office of jurisdiction and automation of the third-person authorization process for large payments. These two action items are included in the design of the Modern Award Processing System.

Question 7: When will VBA implement a VA smart card with biometrics that could specifically preclude the internal employee fraud that occurred in Bay Pines, Atlanta and Manhattan?

Response: The Veterans Benefits Administration (VBA) will implement the standard VA smart card approximately six months after deployment of Windows 2003 servers and Active Directory. The deployment of Windows 2003 servers and Active Directory must be completed first as a necessary precursor to successful use of this type of smart card. It is currently envisioned that the standard VA smart card will be a smart card with PIN (personal identification number). This type of smart card is consistent with government-wide practice to accomplish control and monitoring of sensitive information, work stations, physical facilities, etc.

This advanced security technology as we currently understand it would not have precluded the internal employee fraud that occurred in Bay Pines, Atlanta, or Manhattan as the employees involved in these cases were authorized to perform the system functions used to perpetrate their criminal activities. As recommended by the OIG, VBA has already implemented changes to the Benefits Delivery Network and its replacement system (Modern Award

Processing/VETSNET) to make SSN the employee corporate identifier and link transactions to SSN.

Question 8: Assuming that smart card technology will allow a user to log on to a PC, will the user, after the initial log on, still be required to enter various additional passwords to access other systems or applications (for example, VISTA, CPRS, MyHealtheVet)?

Response: The One-VA ID Card issued through the AAIP project does provide for network based logon using digital credentials. However, the initial deployment of the AAIP card at the first VHA test site (Fayetteville, AR) will allow the user to log onto the network, but will not provide additional sign-on capabilities.

The AAIP project team is testing a "simplified sign-on" process, which when implemented, will allow users easy sign on to applications such as VistA, CPRS and MyHealtheVet. Once testing is complete and successful, this functionality will be implemented in the pilot test sites. After logon, and depending on the status of system integration efforts, users will be able to concurrently logon to other applications. This may occur through web interfaces, or through other forms of single sign on (SSO) technology. Currently, SSO technologies are under a prototype review to specifically identify implementation requirements. Initial results are expected in Q3 of FY05.

Question for Secretary Wu from Chairman Steve Buyer
Subcommittee on Oversight and Investigations
Committee on Veterans Affairs
October 6, 2004
Hearing on VA Smart Card Initiative(s)

1. VA and DoD have spent billions in the last decade developing stove piped electronic medical records that cant exchange or share information. What should the level of interoperability be between DoD and VA smart cards? Does the National Institute of Standards and Technology's Government Smart Card Interoperability Specifications published in July 2003 address this issue?

Answer: We are not involved with those specific projects. Therefore, we are not in a position to say exactly what should be the level of interoperability by those two agencies to conduct their respective missions. The GSC-IS provides a basis for the interoperability of smart cards produced by various vendors. By itself, however, it does not guarantee complete interoperability among divergent applications that may be loaded and run on the smart cards operating system. Many important technical and policy questions (e.g., credential acceptance policy) must still be addressed.

2. Has any specific agency or department been designated with the responsibility of overseeing the development and implementation of NIST's published guidelines?

Answer: Under the Federal Information Security Management Act of 2002, the Director of the Office of Management and Budget has the responsibility to oversee the development and implementation of standards and guidelines by NIST.

3. How does the smart card effort integrate with your planned implementation of single-sign-on technology?

Answer: NIST is not planning or implementing a single sign-on project. In general, GSC defines an interoperable smart card platform for electronic credentials. In single-sign on systems, GSC cards can hold multiple credentials for all the services accessed by the cardholder. The cardholder logs on to the card once, and the card can then seamlessly log the cardholder on to multiple services.

GAO
Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, DC 20548

November 12, 2004

The Honorable Steve Buyer
Chairman, Subcommittee on Oversight and Investigations
Committee on Veterans' Affairs
House of Representatives

Subject: *Electronic Government: Responses to Subcommittee Post-Hearing Questions Concerning the Department of Veterans Affairs' Use of Smart Card Technology*

Dear Mr. Chairman:

This letter responds to your October 15, 2004, request that we answer questions relating to our testimony of October 6, 2004.[1] In that hearing, we discussed the adoption and use of smart cards among federal agencies, including the Department of Veterans Affairs (VA). Your questions, along with our responses, follow.

1. *From what you have observed, do you believe that only one single sign-on application [should] be used by VA system-wide, or is it possible that the VBA and VHA might have different solutions?*

On the basis of our observations to date, we are not yet able to offer a position on whether and how VA should incorporate a single sign-on capability[2] in its overall implementation of smart card technology. Our work thus far has generally included reviews of project documentation describing the department's early actions toward implementing its Authentication and Authorization Infrastructure Project, such as its initial limited deployment of One-VA ID smart cards. However, we have not yet had an opportunity to fully assess all key components and phases of this project, including any plans that VA has for using a single sign-on capability departmentwide or within its specific administrations.

2. *Does the VA have a planned timeline for bringing both smart card and single sign-on capabilities to the entire VA?*

[1] GAO, *Electronic Government: Smart Card Usage is Advancing Among Federal Agencies, Including the Department of Veterans Affairs*, GAO-05-84T (Washington, D.C.: Oct. 6, 2004).

[2] Single sign-on involves using one authentication method to verify the identity of a user while granting access to multiple applications and services.

During our study of VA's adoption and use of smart cards, the department provided documentation on the Authentication and Authorization Infrastructure Project that identified its planned timeline for implementing the One-VA ID smart card. For example, the timeline called for prototype testing of the smart card during pre-implementation from May through August 2004, followed by limited production at selected VA facilities in the United States beginning in October 2004, and the issuance of 500,000 cards with public key infrastructure (PKI) credentials to VA personnel by January 2006. However, based on our work thus far, we are not yet able to state whether VA also has a planned timeline for bringing a single sign-on capability to the department. While VA's chief information officer noted the department's interest in using this authentication method during the October 6, 2004, hearing, the documentation that VA provided to us did not include a timeline for accomplishing this.

- - - - -

In responding to these questions, we relied on previously reported information and agency documentation describing VA's planned activities to adopt and use smart card technology that was compiled in support of our October 6, 2004, testimony. We did not verify the information that VA provided. VA officials reviewed a draft of this letter and agreed with our responses. We performed our work in accordance with generally accepted government auditing standards during October and November 2004.

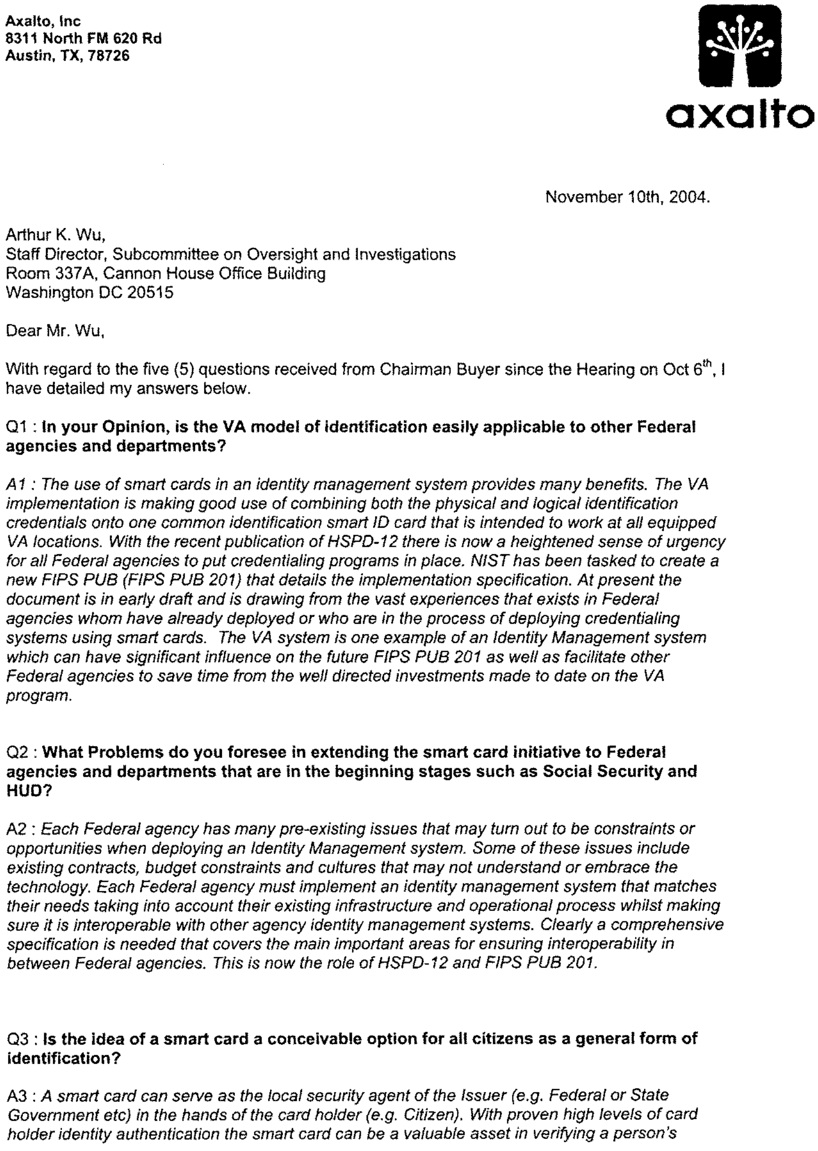
Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-6240 or Valerie Melvin, Assistant Director, at (202) 512-6304. We can also be reached by e-mail at koontzl@gao.gov and melvinv@gao.gov, respectively.

Sincerely yours,

Linda D Koontz

Linda D. Koontz
Director, Information Management Issues

(310727)



Axalto, Inc
8311 North FM 620 Rd
Austin, TX, 78726

November 10th, 2004.

Arthur K. Wu,
Staff Director, Subcommittee on Oversight and Investigations
Room 337A, Cannon House Office Building
Washington DC 20515

Dear Mr. Wu,

With regard to the five (5) questions received from Chairman Buyer since the Hearing on Oct 6th, I have detailed my answers below.

Q1 : **In your Opinion, is the VA model of identification easily applicable to other Federal agencies and departments?**

A1 : *The use of smart cards in an identity management system provides many benefits. The VA implementation is making good use of combining both the physical and logical identification credentials onto one common identification smart ID card that is intended to work at all equipped VA locations. With the recent publication of HSPD-12 there is now a heightened sense of urgency for all Federal agencies to put credentialing programs in place. NIST has been tasked to create a new FIPS PUB (FIPS PUB 201) that details the implementation specification. At present the document is in early draft and is drawing from the vast experiences that exists in Federal agencies whom have already deployed or who are in the process of deploying credentialing systems using smart cards. The VA system is one example of an Identity Management system which can have significant influence on the future FIPS PUB 201 as well as facilitate other Federal agencies to save time from the well directed investments made to date on the VA program.*

Q2 : **What Problems do you foresee in extending the smart card initiative to Federal agencies and departments that are in the beginning stages such as Social Security and HUD?**

A2 : *Each Federal agency has many pre-existing issues that may turn out to be constraints or opportunities when deploying an Identity Management system. Some of these issues include existing contracts, budget constraints and cultures that may not understand or embrace the technology. Each Federal agency must implement an identity management system that matches their needs taking into account their existing infrastructure and operational process whilst making sure it is interoperable with other agency identity management systems. Clearly a comprehensive specification is needed that covers the main important areas for ensuring interoperability in between Federal agencies. This is now the role of HSPD-12 and FIPS PUB 201.*

Q3 : **Is the idea of a smart card a conceivable option for all citizens as a general form of identification?**

A3 : *A smart card can serve as the local security agent of the Issuer (e.g. Federal or State Government etc) in the hands of the card holder (e.g. Citizen). With proven high levels of card holder identity authentication the smart card can be a valuable asset in verifying a person's* *identity back to a reference credential they supplied when they enrolled into the system. In the event that the Federal or State Government wish to address the weak security of existing general forms of identification, smart card technology, in combination with other security technologies can be used to form a much stronger and trusted form of general identification. The smart card can also protect the privacy of the card holder by limiting access to information based on the access rights of the requestor and only when authorized by the card holder.*

Q4 : **Using the guidelines issued under HSPD-12, is a future national database conceivable/desirable?**

A4 : *HSPD-12 defines a "Policy for a Common Identification Standard for Federal Employees and Contractors". As such HSPD-12 instructs each Federal agency to have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the new Standard. It does not mention anything regarding a future national database. As each Federal agency has the responsibility for protecting their employee's privacy it is unnecessary for a national identity or credential database.*

Q5 : **How would individual's right to privacy and protection of liberties be guaranteed?**

A5 : *Smart card technology is able to protect information assets by ensuring that access to information are limited to authorized requestors and data divulgence can be made subject to the card holders consent. Smart Cards can also perform biometric comparisons within the card itself meaning that the enrollment biometric never leaves the card when live captured biometrics are set into the card for matching.*

Yours Sincerely

Neville Pattinson