AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL SECURITY: ID CARDS AND BACKGROUND CHECKS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

APRIL 9, 2008

Serial No. 110–102

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

45–946 PDF WASHINGTON : 2008

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
LAWRENCE HALLORAN, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
CAROLYN B. MALONEY, New York

BRIAN P. BILBRAY, California
TODD RUSSELL PLATTS, Pennsylvania,
JOHN J. DUNCAN, Jr., Tennessee

MICHAEL McCARTHY, *Staff Director*

CONTENTS

	Page
Hearing held on April 9, 2008	1
Statement of:	
Evans, Karen, Administrator for Electronic Government and Information Technology, Office of Management and Budget; Kathy Dillaman, Associate Director of Investigations, Office of Personnel Management; Linda Koontz, Director, Information Management Issues, Government Accountability Office; accompanied by Brenda Farrell, Director, Defense Capabilities and Management, Government Accountability Office; Michael Sade, Acting Deputy Assistant Commissioner, Office of Integrated Technology Service, Federal Acquisition Service, General Services Administration; and Thomas Wiesner, Deputy Chief Information Officer for the Office of the Assistant Secretary for Administration and Management, Department of Labor	8
Dillaman, Kathy	16
Evans, Karen	8
Koontz, Linda	22
Sade, Michael	57
Wiesner, Thomas	64
Zivney, Robert, vice president, marketing, Hirsch Electronics, representing the Security Industry Association; and Benjamin Romero, Chair, Information Technology Association of America Security Clearance Reform Task Group, representing the Security Clearance Reform Coalition	81
Romero, Benjamin	88
Zivney, Robert	81
Letters, statements, etc., submitted for the record by:	
Bilbray, Hon. Brian P., a Representative in Congress from the State of California, prepared statement of	7
Dillaman, Kathy, Associate Director of Investigations, Office of Personnel Management, prepared statement of	18
Evans, Karen, Administrator for Electronic Government and Information Technology, Office of Management and Budget, prepared statement of	11
Koontz, Linda, Director, Information Management Issues, Government Accountability Office, prepared statement of	24
Romero, Benjamin, Chair, Information Technology Association of America Security Clearance Reform Task Group, representing the Security Clearance Reform Coalition, prepared statement of	90
Sade, Michael, Acting Deputy Assistant Commissioner, Office of Integrated Technology Service, Federal Acquisition Service, General Services Administration, prepared statement of	59
Towns, Hon. Edolphus, a Representative in Congress from the State of New York, prepared statement of	3
Wiesner, Thomas, Deputy Chief Information Officer for the Office of the Assistant Secretary for Administration and Management, Department of Labor, prepared statement of	66
Zivney, Robert, vice president, marketing, Hirsch Electronics, representing the Security Industry Association, prepared statement of	84

FEDERAL SECURITY: ID CARDS AND BACKGROUND CHECKS

WEDNESDAY, APRIL 9, 2008

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:10 p.m. in room 2247, Rayburn House Office Building, Hon. Edolphus Towns (chairman of the subcommittee) presiding.

Present: Representatives Towns and Bilbray.

Staff present: Michael McCarthy, staff director; William Jusino, professional staff member; Kwane Drabo, clerk; Janice Spector, minority senior professional staff member; and Benjamin Chance; minority professional staff member.

Mr. TOWNS. The committee will come to order.

Welcome to today's hearing on Federal Security. This hearing will review two important elements of Federal security: identification cards for Federal employees and contractors, and background checks and security clearances.

In 2004, President Bush issued an order titled HSPD–12, adding new requirements in these areas designed to heighten security. In today's hearing we will examine how it is working.

There is a lot at stake with these issues. HSPD–12 helps prevent criminals and terrorists from exploiting Federal ID cards to get access to Federal buildings and computers. Counterfeiters are always hard at work to create phony documents and IDs, so we also have to work hard to stay ahead of them.

I support this kind of effort, but we have to be careful; otherwise, our eagerness to improve security can lead to increased spending without gains in security. That is why I joined with the ranking member, Mr. Bilbray, in asking GAO to review HSPD–12 on the basis of both security and efficiency.

We are releasing their reports today. On the positive side, GAO found that agencies have made a lot of progress in making sure all their employees have the appropriate background checks, and we salute you for that. But GAO has also found that agencies are making very little progress in issuing the new ID cards and, more importantly, are not even using their new security features.

GAO measured progress in eight agencies, and the numbers are grim. At the Department of Commerce, 54,000 employees need cards, but as of December only 23 had been issued. Of the 90,000 employees at the Department of Interior, only 17 had received new

cards. For the 6,000 employees at the Nuclear Regulatory Commission, just 1 card had been issued.

These types of numbers raise serious questions about whether HSPD–12 is working as intended. What is even more troubling is GAO's finding that, even when cards have been issued, the security features are not being used. These features are what makes the new cards so much more secure and also much more expensive—about $80 to issue and to maintain each card in the first year. If agencies do not use these security features, they are just wasting money.

Agencies aren't gaining anything from the new cards if employees just wave them at the security officer instead of putting them through a reader, but they are still spending a lot of money issuing the cards.

Today I hope we can learn more about how to get this program on track so all of this money being spent actually makes the Federal Government more secure, not wasting money.

[The prepared statement of Hon. Edolphus Towns follows:]

HENRY A. WAXMAN, CALIFORNIA,
CHAIRMAN

TOM LANTOS, CALIFORNIA
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
BRIAN HIGGINS, NEW YORK
JOHN A. YARMUTH, KENTUCKY
BRUCE L. BRALEY, IOWA
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
BETTY McCOLLUM, MINNESOTA
JIM COOPER, TENNESSEE
CHRIS VAN HOLLEN, MARYLAND
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
JOHN P. SARBANES, MARYLAND
PETER WELCH, VERMONT

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5051
FACSIMILE (202) 225–4784
MINORITY (202) 225–5074

www.oversight.house.gov

TOM DAVIS, VIRGINIA,
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
DARRELL E. ISSA, CALIFORNIA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. McHENRY, NORTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
BILL SALI, IDAHO
JIM JORDAN, OHIO

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION AND PROCUREMENT

OVERSIGHT HEARING
Federal Security: ID Cards and Background Checks

April 9, 2008,
2:00 p.m. 2247 Rayburn

OPENING STATEMENT
OF CHAIRMAN TOWNS

Welcome to today's hearing on federal security. This hearing will review two important elements of federal security: identification cards for federal employees and contractors, and background checks and security clearances. In 2004, President Bush issued an order titled HSPD-12 adding new requirements in these areas designed to heighten security, and today's hearing will examine how it is working.

There's a lot at stake with these issues. HSPD-12 helps prevent criminals and terrorists from exploiting federal ID cards to get access to federal buildings and computers. Counterfeiters are always hard at work to create phony documents and IDs, so we also have to work hard to stay ahead of them.

I support this kind of effort, but we have to be careful, otherwise our eagerness to improve security can lead to increased spending without gains in security. That is why I

joined with the ranking member Mr. Bilbray in asking GAO to review HSPD-12 on the basis of both security and efficiency. We are releasing their report at today's hearing, and its findings raise a lot of concerns. On the positive side, GAO found that agencies have made a lot of progress in making sure all their employees have the appropriate background checks. But GAO has also found that agencies are making very little progress in issuing the new ID cards, and more importantly, are not even using their new security features.

GAO measured progress in eight agencies, and the numbers are grim. At the Department of Commerce, 54,000 employees need cards, but as of December, only 23 had been issued. Of the 90,000 employees at the Department of the Interior, only 17 had received the new cards. For the 6,000 employees at the Nuclear Regulatory Commission, just one card had been issued. These types of numbers raise serious questions about whether HSPD-12 is working as intended.

What is even more troubling is GAO's finding that even when cards have been issued, the security features are not being used. These features are what make the new cards so much more secure, and also much more expensive – about $80 to issue and maintain each card in the first year. If agencies do not use these security features, they are just wasting money. Agencies aren't gaining anything from the new cards if employees just wave them at a security officer instead of putting them through a reader, but they are still spending a lot of money issuing the cards.

Today I hope we can learn more about how to get this program on track so all this money being spent actually makes the federal government more secure.

Today's hearing will also review delays in background checks and security clearance investigations, a longstanding concern of this Committee. The Office of

Personnel Management performs most investigations for security clearances, as well as the simpler background checks required under HSPD-12. Security clearances have been plagued by long delays and inefficiency for several decades now. It is important to make sure that we only trust national secrets to trustworthy employees. However, delays in issuing security clearances prevent federal employees and contractors from performing the jobs that keep our country safe.

It can take over a year to get a Top Secret clearance, and longer to have one renewed. Delays increase costs to contractors, and these costs are passed to taxpayers. A lack of employees with clearances also leads contractors to recruit federal employees who already have clearances to come work for them instead, and we don't pay as much as they do. We must be diligent about clearance investigations, but we must make sure they are done as quickly as possible. I hope we can hear today about what is being done to reduce the delays in security clearances, and what effect HSPD-12 is having on the investigation process.

With the amount of resources going into these programs, we want to make sure the federal government is getting the most for its time and taxpayer dollars. I look forward to hearing from the witnesses here today as we decide the best ways to address these important security issues.

Mr. TOWNS. At this time I would like to yield to the ranking member, Mr. Bilbray.

Mr. BILBRAY. Thank you, Mr. Chairman. Mr. Chairman, I thank you for this hearing. I appreciate the witnesses showing up this afternoon.

Let me just say that I really have a big concern. When you read the 9/11 Commission's report on the state of national security, one of their No. 1 recommendations right out of the chute was that America has to get serious about secure IDs, not just in the Government but around our country. But by far the Federal Government needs to lead through example.

How many years later are we now saying we are still working on it, we are trying to move the ball ahead? And I think a lot of it is almost reminiscent of what we went through, Mr. Chairman, a couple of years ago with body armor for our troops in Iraq, that people said yes, we want to get it there, we want to deploy it, we want to get it into the hands so that it can be used for protecting our troops. Well, ladies and gentlemen, secure IDs are the body armor of homeland security. It is sometimes the first and sometimes the last line of defense against a terrorist attack, as the 9/11 Commission said.

I would like to just add a degree of urgency to the execution of this directive, that it is not just a nice thing to do, it is an essential thing to do. God forbid if we have another attack. I will tell you right now I can guarantee you that the lack of a uniform enforceable identification system is going to be raised again, and I don't think any of us in this room want to be caught in the position of saying yes, you are right, we just didn't think it was that important. It is of major importance that I do not think we can overstate when it comes down to the fact of knowing who are or who isn't going into our Government facilities and how we are setting examples for States and counties and cities to do the same with their identification system.

So, Mr. Chairman, I appreciate the hearing. I appreciate the chance to be updated on the situation, and hopefully what we can do is learn from our mistakes, raise the degree of urgency, and move forward with a successful implementation plan.

I yield back, Mr. Chairman, and again thank you.

[The prepared statement of Hon. Brian P. Bilbray follows:]

Opening Statement Ranking Member Congressman Brian Bilbray

Subcommittee on Government Management, Organization and Procurement

"Federal Security: ID Cards and Background Checks"

April 9, 2008

I want to thank Chairman Towns for holding this hearing as we continue to monitor the progress of the implementation of HSPD-12 -- the government wide standard for secure and reliable forms of ID. It is vital to ensure that all government facilities and information systems remain secure. We must standardize identification to know who enters these facilities and systems because we have learned how easy it is to obtain bogus credentials.

Given our lack of comprehensive immigration reform it is crucial that we strive to support programs such as REAL ID and HSPD-12. This is a nation at risk that cannot identify its current population. We are unwavering in our support of HSPD—12 and similar programs to standardize secure ID.

Today we will hear from both government and industry experts about the remaining challenges to achieving full implementation of essential secure ID. Because background checks are essential in order to obtain one of these ID's, we will weigh how the current backlog of security clearances may impact implementing the current program.

We will listen to recommendations made by GAO, which were released in a report today, that asks OMB to revise its current approach to how it oversees HSPD-12. We agree with GAO that each agency must have realistic milestones for implementation of the electronic authentication of the ID Card. We would, however, ask GAO to explain very specifically how they recommend OMB move forward. From among the recommendations presented here today, we will be hesitant to embrace methodologies that slow a process that has moved forward, albeit at a slower pace than anticipated.

We are encouraged that the GAO report says GSA officials have taken the initial steps to develop guidelines to reach the goal of achieving interoperability for HSPD-12 across the federal government. That is another step forward—the ID will not fulfill its purpose unless it can be used from agency to agency.

We look forward to weighing the testimony of both government officials and industry experts to find some common ground to keep this important program moving in the right direction.

Mr. TOWNS. Thank you very much.

It is a longstanding policy that we swear our witnesses in, so if you would be kind enough to please stand and raise your right hands.

[Witnesses sworn.]

Mr. TOWNS. Let the record reflect that all of them answered in the affirmative.

We are delighted to have with us today the Honorable Karen Evans, Administrator for Electronic Government and Information Technology, Office of Management and Budget. Welcome.

We are also happy to have Kathy Dillaman, Associate Director of Investigations, Office of Personnel Management. Thank you. Welcome.

Ms. Linda Koontz, Director, Information Management Issues, Government Accountability Office. Thank you. Good to see you again. Accompanied by Ms. Brenda Farrell, Director of Defense Capabilities and Management of the Government Accountability Office.

Also, Mr. Michael Sade, Acting Deputy Assistant Commissioner, Office of Integrated Technology Service, Federal Acquisition Service, General Services Administration. What a title.

Mr. Thomas Wiesner, Deputy Chief Information Officer for the Office of the Assistant Secretary for Administration and Management, Department of Labor.

Why don't we just go right on down the line, starting with you, Ms. Evans, and just come right down the line. Thank you. Thank you so much.

We would like you to summarize in 5 minutes. Of course, we have a light there that comes on. Of course, it starts out as green, and then it turns to caution. That means begin to sum up. And then red means to stop up.

We will start with you, Ms. Evans.

STATEMENTS OF KAREN EVANS, ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; KATHY DILLAMAN, ASSOCIATE DIRECTOR OF INVESTIGATIONS, OFFICE OF PERSONNEL MANAGEMENT; LINDA KOONTZ, DIRECTOR, INFORMATION MANAGEMENT ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; ACCOMPANIED BY BRENDA FARRELL, DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, GOVERNMENT ACCOUNTABILITY OFFICE; MICHAEL SADE, ACTING DEPUTY ASSISTANT COMMISSIONER, OFFICE OF INTEGRATED TECHNOLOGY SERVICE, FEDERAL ACQUISITION SERVICE, GENERAL SERVICES ADMINISTRATION; AND THOMAS WIESNER, DEPUTY CHIEF INFORMATION OFFICER FOR THE OFFICE OF THE ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT, DEPARTMENT OF LABOR

STATEMENT OF KAREN EVANS

Ms. EVANS. Good afternoon, Mr. Chairman and members of the subcommittee. Thank you for inviting me to discuss the administration's implementation of Homeland Security Presidential Directive 12. Protection of our Federal facilities and information systems

is priority for the administration, and my remarks today will focus on the progress we have made in improving security through the implementation of HSPD–12. Details have been included in my written statement.

Prior to HSPD–12 there were wide variations in the quality and security of forms of identification used by Federal employees and contractors to gain access to Federal facilities and information systems. The directive enhances security, increases Government efficiency, reduces identity fraud, and protects personal privacy by establishing a mandatory, Government-wide standard.

The intent of HSPD–12 is to allow agencies to grant access based on risk-based access control decisions; however, we must also protect the personal information of Federal employees and contractors. HSPD–12 implementation is grounded in the longstanding policy framework overseen by OMB, and the agencies must follow existing privacy and security law and policies to ensure our employee and contractor information is protected and appropriately used.

Following the issuance of the FIPS 201 standard, NIST and GSA established a performance and interoperability program to ensure programs are certified with the standard. Currently, there are approximately 350 products and 33 system integrators on the Government certified and approved services and products listing maintained by GSA. NIST and GSA have also issued various publications and guidance to support interoperability and the use of credentials.

It is essential for Federal agencies to be interoperable if we are to significantly improve the security of our Federal systems and facilities.

To ensure agencies are on track with their HSPD plans, OMB has taken steps to closely monitor agency implementation progress and completion of the key activities. In September 2006, OMB asked agencies to submit updated implementation plans. As part of their plans, we requested agencies to include the integration of physical and logical access control systems using the PIV credentials and how they intend to use the capabilities of the credentials to the fullest extent possible to address cyber-security weaknesses and to improve physical access control.

In January 2007 OMB issued guidance requiring quarterly reporting on the status of background investigations and the number of PIV credentials issued. On October 26, 2007, OMB also issued a memorandum providing updated instructions for public reporting of the implementation status, and we requested additional information on background investigation status and major milestones, as outlined in the agency plans.

We are ensuring that agency status is transparent and accessible to the public.

As of March 1, 2008, agencies reported 2.5 million, or 59 percent, of their employees, which includes military personnel, and over 500,000, or 42 percent, of the contractors had completed their background investigations.

The PIV credentials have been issued over 140,000, or 3 percent of employees, and just 36,000 or 3 percent of the contractors.

As part of our oversight role, OMB will continue to use quarterly reporting mechanisms along with agency information technology

budget planning documents to track key performance metrics for HSPD–12 compliance.

Over the past three-and-a-half years the executive branch has made steady progress in achieving the goals of the Presidential directive. HSPD–12 is part of the administration's overall plans to enhance security, and it is closely aligned with other ongoing security initiatives and plans for improving physical security to implement the recommendations of the 9/11 Commission.

With evaluating the physical security, information security, and human resources business practices, the executive branch is applying a consistent, risk-based approach to physical and information systems security that will improve our overall security and reduce cost.

We look forward to working with the members of this committee and appreciate your continued support in improving the security posture. I will be glad to answer questions at the appropriate time.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND
INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, OF
THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

April 9, 2008

Good afternoon, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to discuss the Administration's implementation of Homeland Security Presidential Directive 12 (HSPD-12). Protection of our federal facilities and information systems is a priority for the Administration and my remarks today will focus on the progress we have made in improving security through implementation of HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," issued on August 27, 2004.

Prior to HSPD-12, there were wide variations in the quality and security of forms of identification used by Federal employees and contractors to gain access to federal facilities and information systems. The Directive enhances security, increases Government efficiency, reduces identity fraud, and protects personal privacy by establishing a mandatory, Government-wide standard. Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. HSPD-12 is an important component of agencies' information and physical security programs as it improves the basis for making an access control decision. The Directive requires background investigations and standardized identity credentials for employees and contractors. The use of cryptographic credentials will provide a more accurate determination of identity before access is granted. The identity credentials also enable biometric verification when and if the application requires it. The overall goal is to achieve appropriate security assurance for multiple applications, based on an agency risk determination, by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to information systems.

Government-wide Standard

To implement the goals of HSPD-12, the Administration tasked the Department of Commerce to create a government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. In February 2005, Department of Commerce Secretary Gutierrez signed, and the National Institute of Standards and Technology (NIST) published, the Federal Information Processing Standards (FIPS) 201, "Personal Identity Verification of Federal Employees and Contractors." The final version, FIPS 201-1, was issued in March 2006. This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The FIPS 201-1 standard and several associated special publications provide for interoperability of agency credentials and existing Federal Public Key Infrastructure provides the capability to determine the validity of another agency user's credential. To supplement this capability, the General Services Administration (GSA) developed a technical specification for those agencies wanting to exchange additional identity attributes between Identity Management Systems. This draft specification, issued for interagency comment in March 2008, builds upon the technical specifications already issued by the GSA as well as several NIST guidelines available to assist agencies in determining the types of electronic authentication capabilities to implement for addressing requirements of the Federal Information Security Management Act.

With HSPD-12, agencies are also required to adhere to specific business processes for the issuance of Personal Identity Verification (PIV) credentials including a standardized background check, based on existing Office of Personnel Management (OPM) requirements, to verify employees' and contractors' identities. There has been an existing requirement for federal employees to undergo a background investigation based on Executive Order 10450, "Security Requirements for Government Employees," issued on April 27, 1953. HSPD-12 extends these same background investigation requirements to federal contractors with long-term access to federal facilities and information systems.

We have also directed agencies to take full advantage of the capabilities of the new identity credentials and agencies have been requested to prepare plans outlining their implementation strategies. HSPD-12 and the FIPS 201-1 standard provide the technology component that will enable large scale implementation of existing OMB security and privacy directives, such as requirements for two-factor authentication and encryption of personally-identifiable and sensitive information. Use of PIV credentials will also enable secure information sharing across organizational boundaries through the use of cryptography.

By helping agencies evaluate their physical security, information security, and human resources business practices, the Executive Branch is applying a consistent, risk-based approach to physical and information systems security that will improve our security and reduce cost.

Conformance and Interoperability Testing

It is essential for federal agencies to be interoperable if we are to significantly improve the security of our federal systems and facilities. Without interoperability, we will continue to have wide variations in access control implementations which also greatly increases cost. With HSPD-12, this is the first time the President has mandated interoperability of cryptographic credentials across all departments and agencies.

Following the issuance of the FIPS 201-1 standard, the NIST and GSA established a conformance and interoperability program to ensure products are compliant with the standard and interoperable. Currently, there are approximately 350 products and 33 systems' integrators on the Government Certified and Approved Services and Products Listing maintained by GSA. NIST and GSA have also issued various publications and guidance to support interoperability which can be located on the NIST and GSA websites (http://csrc.nist.gov/ and http://www.smart.gov/awg/). The NIST publications primarily focus on security and interoperability requirements for the credentials while the GSA guidance focuses on both the interoperability of products and HSPD-12 system components. Additionally, NIST developed an automated tool which is available for agencies to test their credentials to ensure compliance with the FIPS 201-1 standard. Initial testing of agency credentials was performed by GSA in January 2007.

Reducing Overall Costs to the Federal Government and Streamlining Processes

Agencies have allocated funds for identity management programs and issued credentials for years. In 2003, OMB analyses of executive agency authentication and identity management efforts concluded that agencies were spending in excess of $160 million in FY 2003 and FY 2004 on potentially inconsistent or agency-unique authentication and identity management infrastructure. Beginning last year, OMB is requiring agencies to report current year expenditures for HSPD-12. Analysis of the initial agency submissions indicates inconsistencies in how agencies reported their costs and OMB is working with the agencies to ensure they report complete information and in accordance with the OMB guidance.

To help reduce the overall federal costs of HSPD-12 implementation, the GSA implemented an HSPD-12 Shared Services Offering to agencies in August 2006. Through the GSA service, credentials are offered at a reduced cost due to economies of scale. Currently, 70 federal departments and agencies are participating in the GSA Shared Services program. The service now includes 64 enrollment centers with over 80 enrollment stations available for agency use. Approximately 120 additional enrollment stations are planned for deployment in FY 2008. We anticipate significant cost avoidance across the federal government as a result of the shared infrastructure and services.

HSPD-12 has also been the impetus to streamline the business process of capturing and transmitting electronic fingerprint files used for screening and adjudication of background investigations for new employees and contractors. The new enrollment stations provide for the electronic transmission of fingerprints to OPM and, for those agencies previously submitting hard copy fingerprints, this will speed the screening and adjudication time required for the hiring process.

Privacy Requirements

HSPD-12 implementation is grounded in the longstanding policy framework overseen by OMB. The intent of HSPD-12 is to allow agencies to grant access based on risk-based access control decisions; however, we must also protect the personal information of federal employees and contractors. Agencies must follow existing privacy and security law and policies to ensure employee and contractor information is protected and appropriately used.

In February 2006, OMB issued Memorandum M-06-06, "Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12," which provides agencies with sample privacy documents to use as models in implementing HSPD-12 in their agencies. The sample documents include:

- System of Records Notice of Personnel Security Files
- System of Records Notice for Identity Management System(s)
- ID Proofing and Registration Privacy Act Statement
- Card Usage Privacy Act Statement
- Privacy Impact Assessment for Personal Identity Verification

Subsequently, in May 2007, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This memorandum re-enforces requirements to protect personally identifiable information.

How Do We Oversee Agency Performance?

To ensure agencies are on track, OMB has taken steps to closely monitor agency implementation progress and the completion of key activities. In September 2006, OMB asked agencies to submit updated HSPD-12 implementation plans. As part of their HSPD-12 implementation plans, we requested agencies document their plans for integrating physical and logical access control systems with the use of PIV credentials. We requested agencies indicate how they intend to use the capabilities of the credentials to the fullest extent possible to address cybersecurity weaknesses and improve physical access control. Additionally, we issued OMB Memorandum M-08-01, "HSPD-12 Implementation Status," on October 23, 2007 directing agencies to either confirm their HSPD-12 implementation plan was still on target or update their plan with a revised schedule by which the agency will meet as soon as possible the requirements of HSPD-12.

In January 2007, OMB issued guidance requiring quarterly reporting on the status of background investigations and number of PIV credentials issued. Beginning March 1, 2007 and each quarter thereafter, agencies were directed to post to their federal agency public website a report on the number of credentials issued. The guidance also requires testing of agency credentials to ensure compliance with the FIPS 201-1 standard published by NIST. Additionally, we asked the President's Council on Integrity and Efficiency to conduct a review of agency processes to ensure they are consistent with HSPD-12 and FIPS 201-1. As a result, several agencies' Inspectors General completed reviews of agency HSPD-12 implementations and provided recommendations to the agencies. On October 26, 2007, OMB also issued a memorandum providing updated instructions for public reporting of HSPD-12 implementation status and we requested additional information on background investigation status and major milestones as outlined in agency HSPD-12 plans. We are ensuring that agency status is transparent and accessible to the public.

Status of Agency Implementations

In accordance with their HSPD-12 implementation plans, by October 27, 2008, agencies are expected to complete background investigations for all existing employees and contractors and ensure their infrastructure and capabilities are in place so they are issuing credentials as standard business practice. Agencies must also continue to complete all additional milestones as indicated in their agency/OMB mutually agreed-upon implementation plans. The current status of agency implementation is as follows:

- On December 31, 2007, OMB released the first aggregate review of agencies' public posting of HSPD-12 implementation status reports. OMB's review and the details of the agency HSPD-12 Implementation Plan reports can be found on the E-gov website (http://www.whitehouse.gov/omb/egov/b-1-information.html.)
- As of March 1, 2008, agencies reported:
    - over 2.5 million or 59% of their employees (which includes military personnel) have completed background investigations
    - over 500,000 or 42% of contractors have completed background investigations
    - over 143,000 or 3% of employees have received PIV credentials
    - over 36,000 or 3% of contractors have received PIV credentials
    - over 900 or 0.8% of other individuals that agencies have identified as requiring credentials based on their long-term access to federal facilities or information systems have received PIV credentials
- In addition to the approximately 180,000 individuals that have received credentials, as of March 31, 141,000 have completed the enrollment process to receive their identity credentials.

Next Steps

As part of our oversight role, OMB will continue to use quarterly reporting mechanisms along with agency information technology budget planning documents to track key performance metrics for HSPD-12 compliance.

Additionally, in anticipation of agencies' plans to integrate the use of PIV credentials with physical access systems, NIST, in consultation with the Interagency Security Committee and several federal agencies, developed Special Publication 800-116, "A Recommendation for the Use of PIV Credentials with Physical Access Control Systems." The publication provides guidelines for securely and cost effectively integrating PIV credentials and readers with physical access control systems. The purpose is to describe a strategy for agencies to enable their physical access control systems to use PIV credentials. The draft publication was released for a 42-day public comment period on April 1, 2008.

Conclusion

Over the past three and a half years, the Executive branch has made steady progress in achieving the goals of the Presidential Directive. HSPD-12 and the FIPS 201-1 standard, when implemented, provide the foundation for identity trust and the ability to streamline business processes to improve authentication processes. The government's implementation and use of PIV credentials will result in a standardized environment for launching a number of new applications and improving the security of federal information systems and facilities.

HSPD-12 is part of the Administration's overall plans to enhance security and is closely aligned with other ongoing security initiatives and plans for improving physical security to implement recommendations of the 9-11 Commission. Once fully implemented, we expect HSPD-12 to significantly improve the federal government's security posture and reduce costs through implementation of standard processes and federated identity management. We continue to build upon our existing efforts to improve security and enhance privacy.

We look forward to working with the members of this Committee and appreciate your continued support in improving the security posture of the federal government.

Mr. TOWNS. Thank you very much, Ms. Evans.

STATEMENT OF KATHY DILLAMAN

Ms. DILLAMAN. Good afternoon. Chairman Towns, members of the subcommittee, it is my privilege to testify today on behalf of the Office of Personnel Management on the implementation of HSPD–12 and the status of the background investigations program.

OPM's mission is to ensure that the Federal Government has an effective work force. To accomplish this mission, we conduct over 2 million background investigations each year for Federal agencies to assist them in making decisions relating to identity verification, basic suitability, and eligible for security clearances.

HSPD–12 requires agencies to initiate, at a minimum, a national agency checks with written inquiries level investigation or any other standard level of investigation required for Federal employment prior to issuance of a PIV card.

The national agency check portion of the investigation includes searches of the investigative files maintained by the Office of Personnel Management, the Department of Defense, the FBI, and a fingerprint-based criminal history check.

Agencies may issue new PIV card after the fingerprint check has been completed, which is typically within the first 24 hours after an investigation is scheduled.

Last year, OPM received 285,000 requests for the NACI level investigation. That was an increase of over 113,000 from the previous year. This type of investigation is almost entirely automated. It includes electronic processes for the exchange of information between OPM and many Federal, State, and local agencies.

Automated letters of inquiry are also sent to former employers, supervisors, educational institutions, and other references to identify potential suitability or security concerns.

The advanced fingerprint check results and the full investigative results may be sent to the requesting agencies electronically, as well.

Given the automated nature of a NACI investigation, the overall impact on OPM's investment program with this increased workload has been minimal, and we have successfully expanded our work force to process the additional workload without negatively impacting on the timeliness of our national security investigations.

This increased workload did, however, have an impact on a number of the records we asked for from Federal, State, and local agencies. We have been working closely with them to increase their processing capacity, automate information exchanges whenever possible, and improve the time required to obtain those necessary searches.

To support adjudication of these investigations, in December 2007, OPM issued interim standards for agencies to apply when determining whether to issue or revoke PIV cards to their employees or contractor personnel. Agencies are now reviewing the standards, and an interagency working group will be formed to address their implementation concerns prior to issuing final standards later this year.

I would also like to provide you with an update of where we are with processing national security investigations. The Intelligence Reform and Terrorism Prevention Act of 2004 set timeliness standards for the overall security clearance process. I am pleased to report that, overall, OPM and clearance granting agencies are meeting and exceeding the standards of completing 80 percent of initial security clearance determinations in an average of 120 days or less. There is no longer a backlog of investigations due to insufficient resources.

To meet the act's standard, we first focused on the timeliness and quality of the agencies' submissions for investigations. By increasing the use of OPM's Web-based electronic questionnaire for investigations processing instead of sending by paper, we have reduced the time required to request investigations to 14 days and dropped the rejection rate to about 7 percent.

Today over 83 percent of all submissions for national security investigations are electronic, not paper, and 14 agencies are submitting all of their requests online.

Within the 120-day standard the act specifically required that 80 percent of the background investigations that support the clearances be completed within an average of 90 days. We are exceeding this goal.

Of the 586,000 investigations OPM opened last year for national security clearances, 80 percent were completed in an average of 67 days.

After completing the investigation, it is returned to the employing agency for adjudication. The act further established a standard for agencies to adjudicate 80 percent of the initial clearances in an average of 30 days or less. Last fiscal year for actions reported, agencies adjudicated 80 percent of the completed investigations in an average of 28 days, which included up to 14 days of mail and handling time between OPM and the Federal security offices.

To streamline and minimize the time required to transmit completed investigations between OPM and the agencies, we have implemented a state-of-the-art imaging system that allows us to transmit completed investigations to agencies electronically, eliminating mail and reducing handling time.

We continuing to optimize the current process by maintaining adequate staffing, building partnerships with information suppliers, and through greater use of information technology. We are also partnering with the Office of the Director of National Intelligence and DOD for more significant reforms to the overall security clearance processes. This reform effort is challenging traditional processing from application through adjudication. The ultimate outcome of this effort will be a Government-wide system that continues to protect national security through more modern processes that are secure, dependable, scaleable, time-, and cost-efficient.

That concludes my remarks. I would be happy to answer any questions you may have.

[The prepared statement of Ms. Dillaman follows:]

STATEMENT OF

Kathy L. Dillaman
Associate Director
Federal Investigative Services Division
Office of Personnel Management

before the

Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement
United States House of Representatives

on

Federal Security: ID Cards and Background Checks

April 9, 2008

Chairman Towns and Members of the Subcommittee, it is my privilege to testify today on behalf of the Office of Personnel Management (OPM) on the implementation of Homeland Security Presidential Directive 12 (HSPD-12) and the status of the background investigation process.

When President George W. Bush issued HSPD-12 on August 27, 2004, he said the policy of the United States is to enhance security, increase Government efficiency, reduce identity theft, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. OPM Director Linda Springer takes that direction seriously and has included in OPM's Strategic and Operational Plan specific goals to ensure OPM provides the guidance and support the agencies need to implement the requirements HSPD-12.

Background

OPM's mission is to ensure the Federal Government has an effective civilian workforce. To accomplish this mission, OPM provides background investigation products and services to Federal agencies to assist them in making decisions relating to identity, suitability, and security clearances. In Fiscal Year 2007, OPM conducted over two million investigations on Federal applicants, employees, military members, and contractor personnel, including almost 300,000 National Agency Checks with Written Inquiries (NACI), the minimum investigation required for identification purposes. The division at OPM responsible for conducting background investigations is the Federal Investigative Services Division (FISD).

The Investigation Process

The HSPD-12 process begins with the agency initiating the National Agency Check with Written Inquiries (NACI) or other OPM or National Security investigation required for Federal

employment. The National Agency Check (NAC) portion of any background investigation includes searches of the investigation databases maintained by OPM, the Department of Defense (DOD), and the FBI, and the fingerprint-based national criminal history check. The agency may issue an interim PIV card after the fingerprint check has been completed. OPM provides agencies with the option to receive the results of the fingerprint check or National Agency Checks in advance of the completed investigation. These services are available to all agencies whether they submit hardcopy or electronic fingerprints.

In Fiscal Year 2007, OPM received 285,000 requests for NACI level investigations – an increase of 40% from Fiscal Year 2006 levels, primarily attributed to implementation of HSPD 12. For the most part, the NACIs are processed through our automated system – the Personnel Investigation Processing System (PIPS). The system includes standard electronic processes for the exchange of information between OPM and Federal, State, and local record systems. It also generates letters of inquiry to former employers, supervisors, educational institutions, and other references to identify potential suitability or security concerns. Returned responses are processed using Optical Mark Reading technology.

The advanced fingerprint checks and full investigation results may be sent to the requesting agency electronically as well. Given the automated nature of the NACI level investigation, the overall impact to OPM's investigations program has been minimal and we have successfully expanded our Federal and contractor workforce to process the additional workloads generated by HSPD 12 without negatively impacting our other national security workloads.

This increased workload did, however, have an impact on the number of record searches requested from Federal, State, and local record providers. We have been working closely with them to increase their processing capacity, automate information exchange processes when possible, and improve the time required to obtain search results.

Adjudication Guidance

OPM is responsible for developing adjudication guidelines for these investigations. On December 18, 2007, OPM issued interim credentialing standards for Federal departments and agencies to use when determining whether to issue or revoke personnel identity verification (PIV) cards to their employees or contractor personnel. Agencies have been asked to review this guidance, assess the impact of implementation and identify any issues yet to be resolved. An interagency working group will be established to address agencies' concerns prior to issuing final standards.

Status of the security clearance and investigation process

The Intelligence Reform and Terrorism Prevention Act of 2004 set timeliness requirements for the initial security clearance and investigation process. To ensure these goals are met, OPM worked closely with the Office of Management and Budget and the security clearance granting

agencies to establish goals for each phase of the process: workload projections, agency submission of investigation requests, the investigations process, and agencies' adjudications processes. Significant progress has been made in these areas to improve the overall timeliness of investigations and adjudications, and we are continuing to work aggressively to resolve any issues that may delay security clearance determinations.

Timeliness and quality of agency submissions of investigations: The first step in improving the timeliness of the investigation and security clearance process is timely and accurate submission of the subject's background information to OPM. The expanded use of OPM's web based electronic Questionnaires for Investigations Processing (e-QIP) which allows applicants to provide their background information security on line instead of submitting a paper form, has improved both processing timeliness and the quality of the information supplied. As of the beginning of Fiscal Year 2008, 83 percent of the submissions for national security investigations were made through e-QIP, with 14 agencies submitting all requests electronically. In addition, all industry submissions for the Department of Defense are requested electronically.

In February 2008, agencies submissions for initial security investigations through e-QIP averaged 14 days meeting the performance goal for this process. Hardcopy submission timeliness averaged 30 days – a significant improvement over the 55 calendar days reported in November 2005. In addition, the rejection rate for electronic submissions is currently 7 percent, close to the performance goal of less than 5 percent.

Investigations Timeliness: The Intelligence Reform Act required 80 percent of background investigations for initial security clearances to be completed within an average of 90 days by 2006. OPM is exceeding this goal. Of the 586,569 initial clearance investigations OPM received during Fiscal Year 2007, 80 percent were completed in an average of 67 days (92 days for 64,722 Top Secret and 63 days for 404,534 Secret/Confidential). As a result of OPM's increased investigation staffing to almost 9,400 Federal and contractor employees, there is no longer a backlog of initial clearance investigations due to insufficient manpower resources. In fact, this staff increase has resulted in the substantial decrease in the time it takes to complete the majority of the background checks submitted to OPM. During October 2006, there were over 98,000 pending initial clearance investigations that were over 180 days in process. As of March 29, 2008, OPM only had 13,365 pending investigations over 180 days in process.

While improving the timeliness of investigations, we have been vigilant in maintaining the quality of those investigations. We have put additional internal quality control processes in place to ensure that the investigations we conduct meet the national investigative standards and the needs of the adjudication community.

Adjudication Timeliness: OPM continues to work with agencies to reduce the time it takes to deliver completed investigations between OPM and the adjudicating agencies, and to record agency adjudication actions in our record system. This includes full implementation of our imaging system to electronically transmit the results of completed investigations to the adjudications facility and linking the agency's in-house record system to OPM's database for electronic updating of their adjudication actions. A good example of how this works is the pilot we started with the Department of the Army in August 2007. To date, over 162,000 completed

investigations have been sent electronically to Army for adjudication action, making the entire process between OPM and Army virtually paperless. During Fiscal Year 2008, we expect other agencies to adopt this method of receiving completed investigations.

Reform Initiatives

In summary, we are continuing to optimize the current process by maintaining adequate staffing, building partnerships with information suppliers, and through greater use of information technology. This year, *EPIC*, which is OPM's suite of automation tools that support the investigations and adjudications process, will allow for total end-to-end paperless processing for those agencies that are prepared to use them.

We are also partnering with the Office of the Director of National Intelligence and the Department of Defense for more significant reforms to the overall security clearance processes. On February 5, 2008, President Bush issued a memorandum to the heads of the Executive Departments and Agencies reaffirming his support in reforming the personnel security clearance program across Government. This reform effort is challenging traditional processing from application through adjudication. The ultimate outcome of this effort will be a Government-wide system that continues to protect national security through more modern processes that are secure, dependable, scalable, and time and cost-efficient.

This concludes my remarks. I would be happy to answer any questions the Subcommittee may have.

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

STATEMENT OF LINDA KOONTZ

Ms. KOONTZ. Good afternoon. Mr. Chairman and members of the subcommittee, I appreciate the opportunity to discuss our work on the Federal Government's progress in implementing Homeland Security Presidential Directive 12 and challenges in the Department of Defense's personnel security clearance process.

Brenda Farrell is with me today. She is responsible for GAO's work on the security clearances and can address any questions that you might have on that subject.

First, I would like to summarize our report on HSPD–12 that is being released today. As you know, the directive was intended to increase the quality and security of identification practices across the Federal Government and called for the establishment of a mandatory, Government-wide standard for secure and reliable forms of identification. Much work has been accomplished to lay the foundations for implementing this directive, which we recognize as a major Government undertaking.

However, agencies have made limited progress in using the full suite of sophisticated electronic capabilities built into these smart card based ID cards. As a result, at the time of our review, agencies had realized only marginal improvements in heightening security. More specifically, the eight agencies we reviewed had generally done basic foundation work, such as completing background checks on most of their employees and contractors, and beginning to acquire essential equipment, such as card readers. However, none of agencies met OMB's goal of issuing ID cards by October 27, 2007, to all employees who had been with the agency 15 years or less and to contractor personnel.

Further, for the limited number of cards that had been issued, agencies generally were not using the electronic authentication capabilities of the cards which are critical to improving security, and instead were primarily relying on visual inspection, much as previous ID cards had been used.

Most agencies we looked at had also not developed detailed plans as to when they would be able to use these critically important capabilities.

This has occurred largely because OMB's implementation strategy has focused on card issuance rather than on agencies establishing complete security systems, of which the new cards are only one part.

We made a number of recommendations to OMB, including that it establish milestones for completing the complete security systems needed to optimize use of the cards and to align acquisition of the cards with the implementation of these systems.

In commenting on our report, OMB neither agreed nor disagreed with these recommendations. However, until OMB takes action to address the issues we identified, agencies will likely continue to make limited progress in using the cards to improve security over Federal facilities and systems.

Regarding personnel security clearances, our past reports have identified delays and impediments in DOD's personnel security

clearance program which maintains about 2.5 million clearances. These longstanding delays resulted in our adding the DOD security clearance program to our high-risk list in 2005.

Over the past few years several positive changes have been made to the clearance processes because of increased congressional oversight, recommendations from our body of work, new legislative and Executive requirements, most notably the passage of the Intelligence Reform and Terrorism Prevention Act of 2004.

An important step forward is the formation of an interagency team that plans to address past impediments and manage security reform efforts. The President has called for this interagency team to provide this reform proposal no later than the end of this month; however, much work remains to be done before a new system can be implemented.

That concludes my summary, and Ms. Farrell and I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Koontz follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Government Management, Organization, and Procurement; Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, April 9, 2008

EMPLOYEE SECURITY

Implementation of Identification Cards and DOD's Personnel Security Clearance Program Need Improvement

Statement of
Linda D. Koontz
Director, Information Management Issues

Brenda S. Farrell
Director, Defense Capabilities and Management

GAO-08-551T

Abbreviations

CHUID	cardholder unique identifier
DHS	Department of Homeland Security
DOD	Department of Defense
DSS	Defense Security Service
FIPS	Federal Information Processing Standard
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
HUD	Department of Housing and Urban Development
ID	identification
MSO	Managed Service Office
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OUSD(I)	The Office of the Under Secretary of Defense (Intelligence)
PIN	personal identification number
PIV	personal identity verification
PKI	public key infrastructure
USDA	U.S. Department of Agriculture

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.

April 9, 2008

GAO
Accountability·Integrity·Reliability
Highlights

Highlights of GAO-08-551T, a testimony to Subcommittee on Government Management, Organization, and Procurement; Committee on Oversight and Government Reform, House of Representatives

EMPLOYEE SECURITY

Implementation of Identification Cards and DOD's Personnel Security Clearance Program Need Improvement

Why GAO Did This Study

In an effort to increase the quality and security of federal identification (ID) practices, the President issued Homeland Security Presidential Directive 12 (HSPD-12) in August 2004. This directive requires the establishment of a governmentwide standard for secure and reliable forms of ID. GAO was asked to testify on its report, being released today, assessing the progress selected agencies have made in implementing HSPD-12. For this report, GAO selected eight agencies with a range of experience in implementing ID systems and analyzed actions these agencies had taken.

GAO was also asked to summarize challenges in the DOD personnel security clearance process. This overview is based on past work including reviews of clearance-related documents. Military servicemembers, federal workers, and industry personnel must obtain security clearances to gain access to classified information. Long-standing delays in processing applications for these clearances led GAO to designate the Department of Defense's (DOD) program as a high-risk area in 2005.

In its report on HSPD-12, GAO made recommendations to the Office of Management and Budget (OMB), to, among other things, set realistic milestones for implementing the electronic authentication capabilities. GAO has also made recommendations to OMB and DOD to improve the security clearance process.

To view the full product, including the scope and methodology, click on GAO-08-551T. For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

What GAO Found

Much work had been accomplished to lay the foundations for implementation of HSPD-12—a major governmentwide undertaking. However, none of the eight agencies GAO reviewed—the Departments of Agriculture, Commerce, Homeland Security, Housing and Urban Development, the Interior, and Labor; the Nuclear Regulatory Commission; and the National Aeronautics and Space Administration—met OMB's goal of issuing ID cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that had been issued, most agencies had not been using the electronic authentication capabilities on the cards and had not developed implementation plans for those capabilities. A key contributing factor for this limited progress is that OMB had emphasized issuance of the cards, rather than full use of the cards' capabilities. Furthermore, agencies anticipated having to make substantial financial investments to implement HSPD-12, since ID cards are considerably more expensive than traditional ID cards. However, OMB had not considered HSPD-12 implementation to be a major new investment and thus had not required agencies to prepare detailed plans regarding how, when, and the extent to which they would implement the electronic authentication mechanisms available through the cards. Until OMB revises its approach to focus on the full use of the capabilities of the new ID cards, HSPD-12's objectives of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

Regarding personnel security clearances, GAO's past reports have documented problems in DOD's program including delays in processing clearance applications and problems with the quality of clearance related reports. Delays in the clearance process continue to increase costs and risk to national security, such as when new DOD industry employees are not able to begin work promptly and employees with outdated clearances have access to classified documents. Moreover, DOD and the rest of the federal government provide limited information to one another on how they individually ensure the quality of clearance products and procedures. While DOD continues to face challenges in timeliness and quality in the personnel security clearance process, high-level government attention has been focused on improving the clearance process.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on the federal government's progress in implementing Homeland Security Presidential Directive 12 (HSPD-12) and challenges with the Department of Defense's (DOD) personnel security clearance process. As you know, in an effort to increase the quality and security of ID and credentialing practices across the federal government, the President issued HSPD-12 in August 2004. This directive ordered the establishment of a mandatory, governmentwide standard for secure and reliable forms of ID for federal government employees and contractors who access government-controlled facilities and information systems. In addition, one of the primary goals of HSPD-12 is to enable interoperability across federal agencies.

In February 2005, the Department of Commerce's National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*. Known as FIPS 201, the standard is divided into two parts. The first part, personal identity verification (PIV)-I, sets out uniform requirements for identity proofing—verifying the identity of individuals applying for official agency credentials—and for issuing credentials, maintaining related information, and protecting the privacy of the applicants. The Office of Management and Budget (OMB), which is responsible for ensuring compliance with the standard, issued guidance directing agencies to implement these requirements, with the exception of the privacy provisions, by October 27, 2005. The second part, PIV-II, specifies the technical requirements for credentialing systems for federal employees and contractors on the basis of interoperable[1] smart cards.[2] OMB directed that by October 27, 2007, PIV credentials

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

[2]Smart cards are plastic devices—about the size of a credit card—that use integrated circuit chips to store and process data, much like a computer. This processing capability distinguishes these cards from traditional magnetic strip cards, which store information but cannot process or exchange data with automated information systems.

be issued to and used by all employees and contractors who have been with the agency for 15 years or less. It also directed that the remainder of the employees be issued cards and begin using their cards no later than October 27, 2008.

At your request, our testimony today summarizes our report, which is being released today.[3] Specifically, the report assessed the progress selected agencies had made in (1) implementing the capabilities of the PIV cards to enhance security and (2) achieving interoperability with other agencies. In addition, you asked us to provide an overview of long-standing challenges that have had a negative effect on DOD's personnel security clearance process. Long-standing delays in processing personnel security clearance applications and other challenges in DOD's personnel security clearance program led us to designate the program as a high risk area in 2005.[4] In preparing this testimony, we relied on our work supporting the report being released today and on our body of work on clearances. Our work was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

Much work had been accomplished to lay the foundations for implementation of HSPD-12, a major governmentwide undertaking. However, agencies had made limited progress in implementing and

[3]GAO, *Electronic Government: Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards*, GAO-08-292 (Washington, D.C.: Feb. 29, 2008).

[4]GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007); and *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: January 2005). The areas on our high-risk list received their designation because they are major programs and operations that need urgent attention and transformation in order to ensure that our national government functions in the most economical, efficient, and effective manner possible.

using PIV cards. The eight agencies we reviewed—the Departments of Agriculture (USDA), Commerce, Homeland Security (DHS), Housing and Urban Development (HUD), the Interior, and Labor; the Nuclear Regulatory Commission (NRC); and the National Aeronautics and Space Administration (NASA)—had generally completed background checks on most of their employees and contractors and established basic infrastructure, such as purchasing card readers. However, none of the agencies met OMB's goal of issuing PIV cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that had been issued, agencies generally had not been using the electronic authentication capabilities on the cards and had not developed implementation plans for those authentication mechanisms. A key contributing factor for why agencies had made limited progress is that OMB, which is tasked with ensuring that federal agencies implement HSPD-12, had emphasized the issuance of the cards, rather than the full use of the cards' capabilities. Furthermore, agencies anticipated having to make substantial financial investments to implement HSPD-12, since PIV cards are considerably more expensive than traditional ID cards. However, OMB does not consider the implementation of HSPD-12 to be a major new investment. As a result, OMB had not directed agencies to prepare detailed plans to support their decisions regarding how, when, and the extent to which they will implement the various electronic authentication capabilities. Furthermore, without implementing the cards' electronic authentication capabilities, agencies will continue to purchase costly PIV cards and use them in the same way as the much cheaper, traditional ID cards they are replacing. Until OMB revises its approach to focus on the full use of card capabilities, HSPD-12's objectives of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

While steps had been taken to enable future interoperability, progress was limited in implementing such capabilities in current systems, partly because key procedures and specifications had not yet been developed to enable electronic cross-agency authentication of cardholders. According to GSA officials, they had taken the initial steps to develop guidance to help enable the exchange of identity

information across agencies, and they planned to complete and issue it by September 2008.

Regarding personnel security clearances, our previous reports documented problems in the Department of Defense's (DOD) program including delays in processing clearance applications and problems with the quality of investigative and adjudicative reports to determine clearance eligibility. As we noted in February 2008, delays in determining the eligibility for a clearance continue.[5] For example, DOD's August 2007 congressionally mandated report on clearances for industry personnel noted that it took 276 days to complete the end-to-end processing of initial top secret clearances in the first 6 months of fiscal year 2007. These delays result in increased costs and risk to national security, such as when new industry employees are not able to begin work promptly and employees with outdated clearances have access to classified documents. Moreover, DOD and the rest of the federal government provide limited information to one another on how they individually ensure the quality of clearance products and procedures which affects reciprocity of clearances. Reciprocity occurs when one government agency fully accepts a security clearance granted by another government agency. In our September 2006 report, we noted that agencies may not reciprocally recognize clearances granted by other agencies because the other agencies may have granted clearances based on inadequate investigations and adjudications.[6] While delays continue in completing the end-to-end processing of security clearances, recent high-level governmentwide attention has been focused on improving the process. For example, in June 2007, an interagency team was established to reform the security clearance process. In addition, on February 5, 2008, the President issued a memorandum calling for aggressive reform efforts of the security clearance process and directed that the interagency team provide an initial reform plan not later than April 30, 2008.

[5] GAO, *DOD Personnel Clearances: Improved Annual Reporting Would Enable More Informed Congressional Oversight*, GAO-08-350 (Washington, D.C.: February 13, 2008).

[6] GAO, *DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve Security Clearance Process*, GAO-06-1070 (Washington, D.C.: September 28, 2006).

We have made numerous recommendations to improve the implementation of both HSPD-12 and the personnel security clearance process. For example, we recommended in our HSPD-12 report that OMB revise its approach to overseeing the implementation of this directive, including establishing realistic milestones for implementation of electronic authentication capabilities and treating HSPD-12 implementation as a major new investment by requiring that each agency develop detailed plans that support its decisions regarding how, when, and the extent to which it will implement the electronic authentication capabilities of the cards.

With regard to our recommendations, OMB officials indicated that they had already provided agencies with adequate guidance or were in the process of doing so. However, among other things, OMB had not provided realistic milestones for the implementation of infrastructure needed to best use the electronic authentication capabilities of the PIV cards, or required agencies to prepare detailed implementation plans. Implementing our recommendations, should help ensure agencies utilize the electronic capabilities of the cards. We discuss the details of OMB's response later on in our statement.

Background

In August 2004, the President issued HSPD-12, which directed the Department of Commerce to develop a new standard for secure and reliable forms of ID for federal employees and contractors to enable a common standard across the federal government by February 27, 2005. The directive defines secure and reliable ID as meeting four control objectives. Specifically, the identification credentials must be

- based on sound criteria for verifying an individual employee's or contractor's identity;
- strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- able to be rapidly authenticated electronically; and

- issued only by providers whose reliability has been established by an official accreditation process.

HSPD-12 stipulates that the standard must include criteria that are graduated from "least secure" to "most secure" to ensure flexibility in selecting the appropriate level of security for each application. In addition, the directive directs agencies to implement, to the maximum extent practicable, the standard for IDs issued to federal employees and contractors in order to gain physical access to controlled facilities and logical access to controlled information systems by October 27, 2005.[7]

FIPS 201: Personal Identity Verification of Federal Employees and Contractors

In response to HSPD-12, NIST published FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*, on February 25, 2005. The standard specifies the technical requirements for PIV systems to issue secure and reliable ID credentials to federal employees and contractors for gaining physical access to federal facilities and logical access to information systems and software applications. Smart cards are a primary component of the envisioned PIV system. The FIPS 201 standard is composed of two parts, PIV-I and PIV-II.

Personal Identity Verification I

PIV-I sets standards for PIV systems in three areas: (1) identity proofing and registration, (2) card issuance and maintenance, and (3) protection of card applicants' privacy. There are many steps to the identity proofing and registration process, such as completing a background investigation of the applicant,[8] conducting and adjudicating a fingerprint check prior to credential issuance, and requiring applicants to provide two original forms of identity source documents from an OMB-approved list of documents.

[7]In August 2005, OMB issued additional guidance to agencies clarifying which elements of the standard for secure and reliable IDs needed to be implemented by October 27, 2005.

[8]Prior to HSPD-12, agencies were generally conducting some form of a background check on their employees, however, the quality and consistency of the background checks varied among agencies. FIPS 201 established a minimum standard that all agencies must meet for conducting background checks on employees and contractors.

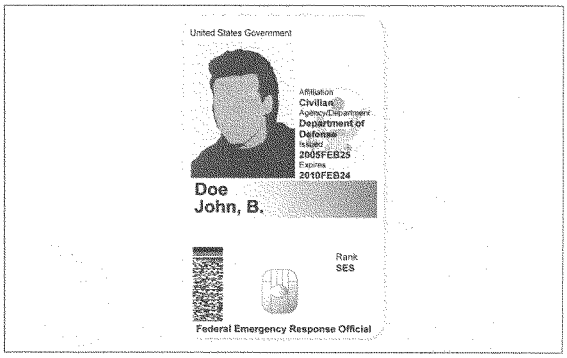
The card issuance and maintenance process should include standardized specifications for printing photographs, names, and other information on PIV cards and for other activities, such as capturing and storing biometric and other data, and issuing, distributing, and managing digital certificates.

Finally, agencies are directed to perform activities to protect the privacy of the applicants, such as assigning an individual to the role of "senior agency official for privacy" to oversee privacy-related matters in the PIV system; providing full disclosure of the intended uses of the PIV card and related privacy implications to the applicants; and using security controls described in NIST guidance to accomplish privacy goals, where applicable.

Personal Identity Verification II

The second part of the FIPS 201 standard, PIV-II, provides technical specifications for interoperable smart card-based PIV systems. The components and processes in a PIV system, as well as the identity authentication information included on PIV cards, are intended to provide for consistent authentication methods across federal agencies. The PIV-II cards (see example in fig. 1) are intended to be used to access all federal physical and logical environments for which employees are authorized.

Figure 1: A PIV Card Showing Major Physical Features



Sources: GAO analysis of FIPS 201 guidance (data). Copyright ©1997 Corel Corp. All rights reserved (seal).

The PIV cards contain a range of features—including photographs, cardholder unique identifiers (CHUID), fingerprints, and Public Key Infrastructure (PKI)[9] certificates—to enable enhanced identity authentication at different assurance levels. To use these enhanced capabilities, specific infrastructure needs to be in place. This infrastructure may include biometric (fingerprint) readers, personal ID number (PIN) input devices, and connections to information systems that can process PKI digital certificates and CHUIDs. Once acquired, these various devices need to be integrated with existing agency systems, such as a human resources system. Furthermore, card readers that are compliant with FIPS 201 need to exchange information with existing physical and logical access control systems in order to enable doors and systems to unlock once a cardholder has been successfully authenticated and access has been granted.

[9] PKI is a system of computers, software, and data that relies on certain cryptographic techniques to protect sensitive communications and transactions.

FIPS 201 includes specifications for three types of electronic authentication that provide varying levels of security assurance.

- The CHUID or visual inspection, provides some confidence.
- A biometric check without the presence of a security guard or attendant at the access point, offers a high level of assurance of the cardholders' identity.
- A PKI check, independently or in conjunction with both biometric and visual authentication, offers a very high level of assurance in the identity of the cardholder.

OMB guidance and FIPS 201 direct agencies to use risk-based methods to decide which type of authentication is appropriate in a given circumstance.

In addition to the three authentication methods, PIV cards also support the use of PIN authentication, which may be used in conjunction with one of these capabilities. For example, the PIN can be used to control access to biometric data on the card when conducting a fingerprint check.

Additional NIST, OMB and GSA Guidance

NIST has issued several publications that provide supplemental guidance on various aspects of the FIPS 201 standard.[10] NIST also developed a suite of tests to be used by approved commercial laboratories to validate whether commercial products for the PIV card and the card interface are in conformation with the standard.

In August 2005, OMB issued a memorandum to executive branch agencies with instructions for implementing HSPD-12 and the new standard. The memorandum specifies to whom the directive applies; to what facilities and information systems FIPS 201 applies; and, as outlined in the following text, the schedule that agencies must adhere to when implementing the standard.

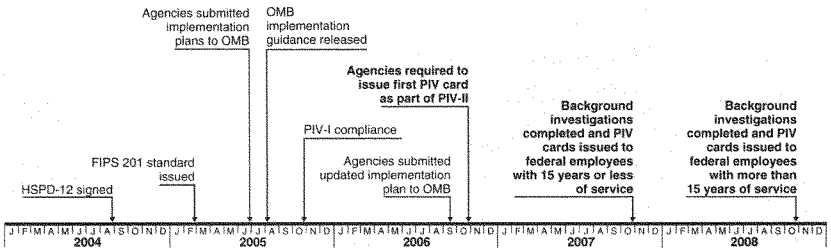
[10] For more information on NIST's guidance see GAO-08-292.

- October 27, 2005—For all new employees and contractors, adhere to the identity proofing, registration, card issuance, and maintenance requirements of the first part (PIV-I) of the standard.
- October 27, 2006—Begin issuing cards that comply with the second part (PIV-II) of the standard and implementing the privacy requirements.
- October 27, 2007—Verify and/or complete background investigations for all current employees and contractors who have been with the agency for 15 years or less. Issue PIV cards to these employees and contractors, and require that they begin using their cards by this date.
- October 27, 2008—Complete background investigations for all individuals who have been federal agency employees for more than 15 years. Issue cards to these employees and require them to begin using their cards by this date.[11]

Figure 2 shows a timeline that illustrates when HSPD-12 and additional guidance was issued as well as the major deadlines for implementing HSPD-12.

[11]In January 2007, OMB issued another memorandum to the chief information officers that further clarifies that employees with more than 15 years of service had to have PIV cards by October 27, 2008. Additionally, on October 23, 2007, OMB issued a memorandum indicating that agencies not meeting OMB's milestones would be directed instead to meet alternate milestones that had been mutually agreed to by the agency and OMB.

Figure 2: Timeline of HSPD-12-Related Activities



Source: GAO analysis of FIPS 201 guidance.

The General Services Administration (GSA) has also provided implementation guidance and product performance and interoperability testing procedures. In addition, GSA established a Managed Service Office (MSO) that offers shared services to federal civilian agencies to help reduce the costs of procuring FIPS 201-compliant equipment, software, and services by sharing some of the infrastructure, equipment, and services among participating agencies. According to GSA, the shared service offering—referred to as the USAccess Program—is intended to provide several services such as producing and issuing the PIV cards. As of October 2007, GSA had 67 agency customers with more than 700,000 government employees and contractors to whom cards would be issued through shared service providers. In addition, as of December 31, 2007, the MSO had installed over 50 enrollment stations with 15 agencies actively enrolling employees and issuing PIV cards. While there are several services offered by the MSO, it is not intended to provide support for all aspects of HSPD-12 implementation. For example, the MSO does not provide services to help agencies integrate their physical and logical access control systems with their PIV systems.

In 2006, GSA's Office of Governmentwide Policy established the interagency HSPD-12 Architecture Working Group, which is intended to develop interface specifications for HSPD-12 system interoperability across the federal government. As of July 2007, the

group had issued 10 interface specification documents, including a specification for exchanging data between an agency and a shared service provider.

Previously Reported FIPS 201 Implementation Challenges

In February 2006, we reported that agencies faced several challenges in implementing FIPS 201, including constrained testing time frames and funding uncertainties as well as incomplete implementation guidance.[12] We recommended that OMB monitor agencies' implementation process and completion of key activities. In response to this recommendation, beginning on March 1, 2007, OMB directed agencies to post to their public Web sites quarterly reports on the number of PIV cards they had issued to their employees, contractors, and other individuals. In addition, in August 2006, OMB directed each agency to submit an updated implementation plan.

We also recommended that OMB amend or supplement governmentwide guidance pertaining to the extent to which agencies should make risk-based assessments regarding the applicability of FIPS 201. OMB has not yet implemented this recommendation.

DOD Personnel Security Clearance Program Has Been Designated as a GAO High-Risk Area

Military servicemembers, federal workers, and industry personnel must obtain security clearances to gain access to classified information. Clearances are categorized into three levels: top secret, secret, and confidential. The level of classification denotes the degree of protection required for information and the amount of damage that unauthorized disclosure could reasonably cause to national security. The degree of expected damage that unauthorized disclosure could reasonably be expected to cause is "exceptionally

[12] GAO, *Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, GAO-06-178 (Washington, D.C.: Feb. 1, 2006).

grave damage" for top secret information, "serious damage" for secret information, and "damage" for confidential information.[13]

We designated DOD's personnel security clearance program a high-risk area in January 2005[14] and continued that designation in the updated list of high-risk areas that we published in 2007.[15] We identified this program as a high-risk area because of long-standing delays in determining clearance eligibility and other challenges. DOD represents about 80 percent of the security clearances adjudicated by the federal government and problems in the clearance program can negatively affect national security. For example, delays in renewing security clearances for personnel who are already doing classified work can lead to a heightened risk of unauthorized disclosure of classified information. In contrast, delays in providing initial security clearances for previously non-cleared personnel can result in other negative consequences, such as additional costs and delays in completing national security-related contracts, lost opportunity costs, and problems retaining the best qualified personnel.

DOD's Office of the Under Secretary of Defense for Intelligence [OUSD(I)] has responsibility for determining eligibility for clearances for servicemembers, DOD civilian employees, and industry personnel performing work for DOD and 23 other federal

[13]5 C.F.R. § 1312.4 (2007).

[14]GAO-05-207.

[15]GAO-07-310.

agencies, and employees in the federal legislative branch.[16] That responsibility includes obtaining background investigations, primarily through the Office of Personnel Management (OPM). Within DOD, government employees use the information in OPM-provided investigative reports to determine clearance eligibility of clearance subjects.

Recent significant events affecting the clearance program of DOD and other federal agencies include the passage of the Intelligence Reform and Terrorism Prevention Act of 2004[17] and the issuance of the June 2005 Executive Order 13381, "Strengthening Processes Relating to Determining Eligibility for Access to Classified National Security Information." The act included milestones for reducing the time to complete clearances, general specifications for a database on security clearances, and requirements for reciprocity of clearances. Among other things, the executive order established as policy that agency functions relating to determining eligibility for access to classified national security information shall be appropriately uniform, centralized, efficient, effective, timely, and reciprocal and provided that the Director of OMB would ensure the policy's effective implementation.

[16]DOD, *National Industrial Security Program: Operating Manual*, DOD 5220.22-M (Feb. 28, 2006), notes that heads of agencies are required to enter into agreements with the Secretary of Defense for the purpose of rendering industrial security services. The following 23 departments and agencies have entered into such agreements: (1) National Aeronautics and Space Administration, (2) Department of Commerce, (3) General Services Administration, (4) Department of State, (5) Small Business Administration, (6) National Science Foundation, (7) Department of the Treasury, (8) Department of Transportation, (9) Department of the Interior, (10) Department of Agriculture, (11) Department of Labor, (12) Environmental Protection Agency, (13) Department of Justice, (14) Federal Reserve System, (15) Government Accountability Office, (16) U.S. Trade Representative, (17) U.S. International Trade Commission, (18) U.S. Agency for International Development, (19) Nuclear Regulatory Commission, (20) Department of Education, (21) Department of Health and Human Services, (22) Department of Homeland Security, and (23) Federal Communications Commission.

[17]Pub. L. No. 108-458 (2004).

Limited Progress Had Been Made in Implementing PIV Cards and in Using Their Full Capabilities

Agencies had made limited progress in implementing and using PIV cards. While the eight agencies we reviewed had generally taken steps to complete background checks on most of their employees and contractors and establish basic infrastructure, such as purchasing card readers, none of the agencies met OMB's goal of issuing PIV cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that had been issued, agencies generally had not been using the electronic authentication capabilities on the cards. A key contributing factor for why agencies had made limited progress in adopting the use of PIV cards is that OMB, which is tasked with ensuring that federal agencies implement HSPD-12, focused agencies' attention on card issuance, rather than on full use of the cards' capabilities. Until OMB revises its approach to focus on the full use of card capabilities, HSPD-12's objective of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

While Agencies Had Generally Completed Background Checks and Established Basic Infrastructure, They Were Not Using the Electronic Authentication Capabilities of PIV Cards to Enhance Security

As we have previously described, by October 27, 2007, OMB had directed federal agencies to issue PIV cards and require PIV card use by all employees and contractor personnel who have been with the agency for 15 years or less. HSPD-12 requires that the cards be used for physical access to federally controlled facilities and logical access to federally controlled information systems. In addition, to issue cards that fully meet the FIPS 201 specification, basic infrastructure—such as ID management systems, enrollment stations, PKI, and card readers—will need to be put in place. OMB also directed that agencies verify and/or complete background investigations by this date for all current employees and contractors who have been with the agency for 15 years or less.

Agencies had taken steps to complete background checks that were directed by OMB, on their employees and contractors and establish basic infrastructure to help enable the use of PIV capabilities. For example, Commerce, Interior, NRC, and USDA had established agreements with GSA's MSO to use its shared infrastructure, including its PKI, and enrollment stations. Other agencies, including DHS, HUD, Labor, and NASA—which chose not to use GSA's shared services offering—had acquired and implemented other basic elements of infrastructure, such as ID management systems, enrollment stations, PKI, and card readers.

However, none of the eight agencies had met the October 2007 deadline regarding card issuance. In addition, for the limited number of cards that had been issued, agencies generally had not been using the electronic authentication capabilities on the cards. Instead, for physical access, agencies were using visual inspection of the cards as their primary means to authenticate cardholders. While it may be sufficient in certain circumstances—such as in very small offices with few employees—in most cases, visual inspection will not provide an adequate level of assurance. OMB strongly recommends minimal reliance on visual inspection. Also, seven of the eight agencies we reviewed had not been using the cards for logical access control.

Furthermore, most agencies did not have detailed plans in place to use the various authentication capabilities. For example, as of October 30, 2007, Labor had not yet developed plans for implementing the electronic authentication capabilities on the cards. Similarly, Commerce officials stated that they would not have a strategy or time frame in place for using the electronic authentication capabilities of PIV cards until June 2008.

Table 1 provides details about the progress each of the eight agencies had made as of December 1, 2007.

Table 1: Agencies' Progress in Implementing Background Checks and Basic Infrastructure and in Using the PIV Cards for Physical and Logical Access Control as of December 1, 2007

	Commerce	Labor	Interior	HUD	DHS	NRC	USDA	NASA
Background investigations and basic infrastructure								
Number of PIV-compliant cards issued (total population requiring PIV cards)[a]	23 (54,420)	10,146 (17,707)	17[b] (90,034)	2,192 (9,335)	N/A[c]	1 (6,245)	313[d] (162,000)	136 (75,467)
Completed background investigations (total population requiring background investigations)[a]	52,246 (54,420)	14,327 (17,707)	83,363[b] (90,034)	6,234 (9,335)	N/A[c]	6,021 (6,245)	99,735[d] (162,000)	38,922 (75,467)
Established an ID management system	●[e]	●	●[e]	●	●	●[e]	●[e]	●
Established enrollment stations	●[e]	●	●[e]	●	●	●[e]	●[e]	●
Established a PKI	●[e,f]	●	●[e]	●	●	●	●[e]	●
Purchased card readers	○	○	●	●	●	●	●	●
Use for physical access								
Used visual inspection to authenticate	●	●	N/A	●	●	●	●	●
Used CHUID to authenticate	○	○	○	●	○	○	○	●
Used PKI to authenticate	○	○	○	○	○	○	○	○
Used biometrics to authenticate	○	○	○	○	○	○	○	○
Use for logical access								
Used CHUID to authenticate	○	○	○	○	○	○	○	○
Used PKI certificates to authenticate	○	○	○	○	○	○	○	○
Used biometrics to authenticate	○	○	○	○	○	○	○	○

Legend: ● implemented ○ not implemented N/A information not available

Source: GAO analysis of documentation provided by agency officials.

[a]These data are as reported by the agencies.

[b]Interior had initially issued 17 cards using an independent provider of cards and services. In August 2007, Interior decided to change its approach and use GSA's shared services offering. These 17 cards expired on October 27, 2007. As of November 2007, Interior had not been issued any new cards from GSA.

[c]According to DHS officials, the public release of the total number of employees requiring and carrying DHS PIV cards could pose a security risk.

[d]The number of cards issued for USDA is as of November 30, 2007, and the number of background checks completed is as of August 31, 2007. Officials did not provide us with figures for December 1, 2007.

[e]This infrastructure is being supplied by GSA's MSO.

[f]Most of Commerce's component agencies plan to use the PKI provided by GSA's MSO. However, the Patent and Trademark Office and the National Oceanic and Atmospheric Administration use their own PKI services.

OMB's Focus on Near-Term Card Issuance Hindered Progress in Achieving the HSPD-12 Objectives

A key contributing factor to why agencies had made limited progress is that OMB—which is tasked with ensuring that federal agencies implement HSPD-12—had emphasized the issuance of the cards, rather than the full use of the cards' capabilities. Specifically, OMB's milestones did not focused on implementation of the electronic authentication capabilities that are available through PIV cards, and had not set acquisition milestones that would coincide with the ability to make use of these capabilities. Furthermore, despite the cost of the cards and associated infrastructure, OMB had not treated the implementation of HSPD-12 as a major new investment and had not ensured that agencies have guidance to ensure consistent and appropriate implementation of electronic authentication capabilities across agencies. Until these issues are addressed, agencies may continue to acquire and issue costly PIV cards without using their advanced capabilities to meet HSPD-12 goals.

OMB's Implementation Milestones Have Been Narrowly Focused

While OMB had established milestones for near-term card issuance, it had not established milestones to require agencies to develop detailed plans for making the best use of the electronic authentication capabilities of PIV cards. Consequently, agencies had concentrated their efforts on meeting the card issuance deadlines. For example, several of the agencies we reviewed choose to focus their efforts on meeting the next milestone—that cards be issued to all employees and contractor personnel and be in use by October 27, 2008. Understandably, meeting this milestone is perceived to be more important than making optimal use of the cards' authentication capabilities, because card issuance is the measure that OMB is monitoring and asking agencies to post on their public Web sites.

The PIV card and the services involved in issuing and maintaining the data on the card, such as the PKI certificates, are costly. For example, PIV cards and related services offered by GSA through its shared service offering cost $82 per card for the first year and $36 per card for each of the remaining 4 years of the card's life. In

contrast, traditional ID cards with limited or no electronic authentication capabilities cost significantly less. Therefore, agencies that do not implement electronic authentication techniques are spending a considerable amount per card for capabilities that they are not able to use. A more economical approach would be to establish detailed plans for implementing the technical infrastructure necessary to use the electronic authentication capabilities on the cards and time the acquisition of PIV cards to coincide with the implementation of this infrastructure.

Without OMB focusing its milestones on the best use of the authentication capabilities available through PIV cards, agencies are likely to continue to implement minimum authentication techniques and not be able to take advantage of advanced authentication capabilities.

OMB Had Not Considered HSPD-12 Implementations to Be a Major New Investment

Before implementing major new systems, agencies are generally directed to conduct thorough planning to ensure that costs and time frames are well understood and that the new systems meet their needs. OMB establishes budget justification and reporting requirements for all major information technology investments. Specifically, for such investments, agencies are directed to prepare a business case—OMB Exhibit 300—which is supported by a number of planning documents that are essential in justifying decisions regarding how, when, and the extent to which an investment would be implemented.

However, OMB determined that because agencies had ID management systems in place prior to HSPD-12 and that the directive only directed agencies to "standardize" their systems. the implementation effort did not constitute a new investment. According to an OMB senior policy analyst, agencies should be able to fund their HSPD-12 implementations through existing resources and should not need to develop a business case or request additional funding.

While OMB did not direct agencies to develop business cases for HSPD-12 implementation efforts, PIV card systems are likely to represent significant new investments at several agencies. For

example, agencies such as Commerce, HUD, and Labor had not implemented PKI technology prior to HSPD-12, but they are now directed to do so. In addition, such agencies' previous ID cards were used for limited purposes and were not used for logical access. These agencies had no prior need to acquire or maintain card readers for logical access control or to establish connectivity with their ID management systems for logical access control and, consequently, had previously allocated very little money for the operations and maintenance of these systems. For example, according to Labor officials, operations and maintenance costs for its pre-HSPD-12 legacy system totaled approximately $169,000, while its fiscal year 2009 budget request for HSPD-12 implementation is approximately $3 million—17 times more expensive.

While these agencies recognized that they are likely to face substantially greater costs in implementing PIV card systems, they had not always thoroughly assessed all of the expenses they are likely to incur. For example, agency estimates may not have included the cost of implementing advanced authentication capabilities where they are needed. The extent to which agencies need to use such capabilities could significantly impact an agency's cost for implementation.

While the technical requirements of complying with HSPD-12 dictated that a major new investment be made, generally, agencies had not been directed by OMB to take the necessary steps to thoroughly plan for these investments. For example, six of the eight agencies we reviewed had not developed detailed plans regarding their use of PIV cards for physical and logical access controls. In addition, seven of the eight agencies had not prepared cost-benefit analyses that weighed the costs and benefits of implementing different authentication capabilities. Without treating the implementation of HSPD-12 as a major new investment by requiring agencies to develop detailed plans based on risk-based assessments of agencies' physical and logical access control needs that support the extent to which electronic authentication capabilities are to be implemented, OMB will continue to limit its ability to ensure that agencies properly plan and implement HSPD-12.

OMB Had Not Provided Guidance for Determining Which PIV Card Authentication Capabilities to Implement for Physical and Logical Access Controls

Another factor contributing to agencies' limited progress is that OMB had not provided guidance to agencies regarding how to determine which electronic authentication capabilities to implement for physical and logical access controls. While the FIPS 201 standard describes three different assurance levels for physical access (some, high, and very high confidence) and associates PIV authentication capabilities with each level, it is difficult for agencies to link these assurance levels with existing building security assurance standards that are used to determine access controls for facilities. The Department of Justice has developed standards for assigning security levels to federal buildings, ranging from level I (typically, a leased space with 10 or fewer employees, such as a military recruiting office) to level V (typically, a building, such as the Pentagon or Central Intelligence Agency headquarters, with a large number of employees and a critical national security mission). While there are also other guidelines that agencies could use to conduct assessments of their buildings, several of the agencies we reviewed use the Justice guidance to conduct risk assessments of their facilities.

Officials from several of the agencies we reviewed indicated that they had not been using the FIPS 201 guidance to determine which PIV authentication capabilities to use for physical access because they had not found the guidance to be complete. Specifically, they were unable to determine which authentication capabilities should be used for the different security levels. The incomplete guidance has contributed to several agencies—including Commerce, DHS, and NRC—not reaching decisions on what authentication capabilities they were going to implement.

More recently, NIST has begun developing guidelines for applying the FIPS 201 confidence levels to physical access control systems. However, this guidance has not yet been completed and was not available to agency officials when we were conducting our review.

Agencies also lacked guidance regarding when to use the enhanced authentication capabilities for logical access control. Similar to physical access control, FIPS 201 describes graduated assurance

levels for logical access (some, high, and very high confidence) and associates PIV authentication capabilities with each level. However, as we have previously reported, neither FIPS 201 nor supplemental OMB guidance provides sufficient specificity regarding when and how to apply the standard to information systems.[18] For example, such guidance does not inform agencies how to consider the risk and level of confidence needed when different types of individuals require access to government systems, such as a researcher uploading data through a secure Web site or a contractor accessing government systems from an off-site location.

Until complete guidance is available, agencies will likely continue either to delay in making decisions on their implementations or to make decisions that may need to be modified later.

Efforts Are Under Way to Address the Limited Progress Made in Achieving Interoperability to Enable Cross-Agency Authentication of Cardholders

As defined by OMB, one of the primary goals of HSPD-12 is to enable interoperability across federal agencies. As we have previously reported, prior to HSPD-12, there were wide variations in the quality and security of ID cards used to gain access to federal facilities.[19] To overcome this limitation, HSPD-12 and OMB guidance direct that ID cards have standard features and means for authentication to enable interoperability among agencies.

While steps had been taken to enable future interoperability, progress had been limited in implementing such capabilities in current systems, partly because key procedures and specifications had not yet been developed. As we have previously stated, NIST established conformance testing for the PIV card and interface, and GSA established testing for other PIV products and services to help enable interoperability. In addition, the capability exists for

[18]GAO-06-178.

[19]GAO-06-178.

determining the validity and status of a cardholder from another agency via PKI. However, procedures and specifications to enable cross-agency interoperability using the CHUID—which is expected to be more widely used than PKI—had not been established. While PIV cards and FIPS 201-compliant readers may technically be able to read the information encoded on any PIV card—including cards from multiple agencies—this functionality is not adequate to allow one agency to accept another agency's PIV card, because there is no common interagency framework in place for agencies to electronically exchange status information on PIV credentials. For example, the agency that issued a PIV card could revoke the cardholder's authorization to access facilities or systems if the card is lost or if there has been a change in the cardholder's employment status. The agency attempting to process the card would not be able to access this information because a common framework to electronically exchange status information does not exist. The interfaces and protocols that are needed for querying the status of cardholders have not yet been developed.

In addition, procedures and policies had not been established for sharing information on contractor personnel who work at multiple federal agencies. Without such procedures and policies, agencies will issue PIV cards to their contractor staff for access only to their own facilities. Contractors who work at multiple agencies may need to obtain separate PIV cards for each agency.

GSA recognized the need to address these issues and has actions under way to do so. According to GSA, the Federal Identity Credentialing Committee is developing guidance on the issuance and maintenance of PIV cards to the contractor community. GSA is also developing a standard specification that will enable interoperability in the exchange of identity information among agencies. According to GSA officials, they plan to complete and issue guidance by the end of September 2008. Additionally, NIST is planning to issue an update to a special publication that focuses on interfaces for PIV systems. Such guidance should help enable agencies to establish cross-agency interoperability—a primary goal of HSPD-12.

Implementation of GAO Recommendations Should Help Achieve the Objectives of HSPD-12

To help ensure that the objectives of HSPD-12 are achieved, we made several recommendations in our report. First, we recommended that OMB establish realistic milestones for full implementation of the infrastructure needed to best use the electronic authentication capabilities of PIV cards in agencies. In commenting on a draft of our report, OMB stated that its guidance requires agencies to provide milestones for when they intend to leverage the capabilities of PIV credentials. However, in order to ensure consistent governmentwide implementation of HSPD-12, it is important for OMB to establish such milestones across agencies, rather than to allow individual agencies to choose their own milestones.

Next, we recommended that OMB require each agency to develop a risk-based, detailed plan for implementing electronic capabilities. OMB stated that previous guidance required agencies to provide milestones for when they plan to fully leverage the capabilities of PIV credentials for physical and logical access controls. However, agencies were required to provide only the dates they plan to complete major activities, and not detailed, risk-based plans. Until OMB requires agencies to implement such plans, OMB will be limited in its ability to ensure agencies make the best use of their cards' electronic authentication capabilities.

We also recommended that OMB require agencies to align the acquisition of PIV cards with plans for implementing the cards' electronic authentication capabilities. In response, OMB stated that HSPD-12 aligns with other information security programs. While OMB's statement is correct, it would be more economical for agencies to time the acquisition of PIV cards to coincide with the implementation of the technical infrastructure necessary for enabling electronic authentication techniques. This approach has not been encouraged by OMB, which instead measures agencies primarily on how many cards they issue.

Lastly, we recommended that OMB ensure guidance is developed that maps existing physical security guidance to FIPS 201 guidance. OMB stated that NIST is in the process of developing additional guidance to clarify the relationship between facility security levels and PIV authentication levels. In March 2008, NIST released a draft of this guidance to obtain public comments.

Long-standing Challenges Exist in DOD's Personnel Security Clearance Program

In our previous reports, we have also documented a variety of problems present in DOD's personnel security clearance program. Some of the problems that we noted in our 2007 high-risk report included delays in processing clearance applications and problems with incomplete investigative and adjudicative reports to determine clearance eligibility. Delays in the clearance process continue to increase costs and risk to national security, such as when new industry employees are not able to begin work promptly and employees with outdated clearances have access to classified documents. Moreover, DOD and the rest of the federal government provide limited information to one another on how they individually ensure the quality of clearance products and procedures. While DOD continues to face challenges in timeliness and quality in the personnel security clearance process, high-level governmentwide attention has been focused on improving the security clearance process.

Delays in Clearance Processes Continue to Be a Challenge

As we noted in February 2008,[20] delays in the security clearance process continue to increase costs and risk to national security. An August 2007 DOD report to Congress noted that delays in processing personnel security clearances for industry have been reduced, yet that time continues to exceed requirements established by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

[20]GAO, *DOD Personnel Clearances: DOD Faces Multiple Challenges in Its Efforts to Improve Clearance Processes for Industry Personnel*, GAO-08-470T (Washington, D.C.: Feb. 13, 2008).

The act currently requires that adjudicative agencies make a determination on at least 80 percent of all applications for a security clearance within an average of 120 days after the date of receipt of the application, with 90 days allotted for the investigation and 30 days allotted for the adjudication. However, DOD's August 2007 report on industry clearances stated that, during the first 6 months of fiscal year 2007, the end-to-end processing of initial top secret clearances took an average of 276 days; renewal of top secret clearances, 335 days; and all secret clearances, 208 days.[21]

We also noted in February 2008,[22] that delays in clearance processes can result in additional costs when new industry employees are not able to begin work promptly and increased risks to national security because previously cleared industry employees are likely to continue working with classified information while the agency determines whether they should still be eligible to hold a clearance. To improve the timeliness of the clearance process, we recommended in September 2006 that OMB establish an interagency working group to identify and implement solutions for investigative and adjudicative information-technology problems that have resulted in clearance delays. In commenting on our recommendation, OMB's Deputy Director for Management stated that the National Security Council's Security Clearance Working Group had begun to explore ways to identify and implement improvements to the process.

DOD and the Rest of the Government Provide Limited Information on How to Ensure the Quality of Clearance Products and Procedures

As we reported in February 2008,[23] DOD and the rest of the federal government provide limited information to one another on how they individually ensure the quality of clearance products and procedures. For example, DOD's August 2007 congressionally

[21]DOD, *Annual Report to Congress on Personnel Security Investigations for Industry and the National Industrial Security Program* (August 2007).

[22]GAO-08-470T.

[23]GAO, *DOD Personnel Clearances: Improved Annual Reporting Would Enable More Informed Congressional Oversight*, GAO-08-350 (Washington, D.C.: Feb. 13, 2008).

mandated report on clearances for industry personnel documented improvements in clearance processes but was largely silent regarding quality in clearance processes. While DOD described several changes to the processes and characterized the changes as progress, the department provided little information on (1) any measures of quality used to assess clearance processes or (2) procedures to promote quality during clearance investigation and adjudication processes. Specifically, DOD reported that the Defense Security Service, DOD's adjudicative community, and OPM are gathering and analyzing measures of quality for the clearance processes that could be used to provide the national security community with a better product. However, the DOD report did not include any of those measures.

In September 2006, we reported[24] that while eliminating delays in clearance processes is an important goal, the government cannot afford to achieve that goal by providing investigative and adjudicative reports that are incomplete in key areas. We additionally reported that the lack of full reciprocity—when one government agency fully accepts a security clearance granted by another government agency—is an outgrowth of agencies' concerns that other agencies may have granted clearances based on inadequate investigations and adjudications. Without fuller reciprocity of clearances, agencies could continue to require duplicative investigations and adjudications, which result in additional costs to the federal government. In the report we issued in February 2008, we recommended that DOD develop measures of quality for the clearance process and include them in future reports to Congress. Statistics from such measures would help to illustrate how DOD is balancing quality and timeliness requirements in its personnel security clearance program. DOD concurred with that recommendation, indicating it had developed a baseline performance measure of the quality of investigations and adjudications and was developing methods to collect information using this quality measure.

[24]GAO, *DOD Personnel Clearances: Additional OMB Actions Are Needed to Improve the Security Clearance Process*, GAO-06-1070 (Washington, D.C.: Sept. 28, 2006).

Recent High-Level Governmentwide Attention Has Been Focused On Improving the Security Clearance Process

In February 2008, we reported[25] that while DOD continues to face timeliness and quality challenges in the personnel security clearance program, high-level governmentwide attention has been focused on improving the security clearance process. For example, we reported that OMB's Deputy Director of Management has been responsible for a leadership role in improving the governmentwide processes since June 2005. During that time, OMB has overseen, among other things, the growth of OPM's investigative workforce and greater use of OPM's automated clearance-application system. In addition, an August 9, 2007, memorandum from the Deputy Secretary of Defense indicates that DOD's clearance program is drawing attention at the highest levels of the department. Streamlining security clearance processes is one of the 25 DOD transformation priorities identified in the memorandum.

Another indication of high-level government attention we reported in February 2008 is the formation of an interagency security clearance process reform team in June 2007. Agencies included in the governmentwide effort are OMB, the Office of the Director of National Intelligence, DOD, and OPM. The team's memorandum of agreement indicates that it seeks to develop, in phases, a reformed DOD and intelligence community security clearance process that allows the granting of high-assurance security clearances in the least time possible and at the lowest reasonable cost. The team's July 25, 2007, terms of reference indicate that the team plans to deliver "a transformed, modernized, fair, and reciprocal security clearance process that is universally applicable" to DOD, the intelligence community, and other U.S. government agencies.

A further indication of high level government attention is a memorandum issued by the President on February 5, 2008 which called for aggressive efforts to achieve meaningful and lasting reform of the processes to conduct security clearances. In the memorandum, the President acknowledged the work being

[25]GAO-08-350.

performed by the interagency security clearance process reform team and directed that the team submit to the President an initial reform proposal not later than April 30, 2008.

In closing, OMB, GSA, and NIST have made significant progress in laying the foundation for implementation of HSPD-12. However, agencies did not meet OMB's October 2007 milestone for issuing cards and most have made limited progress in using the advanced security capabilities of the cards that have been issued. These agency actions have been largely driven by OMB's guidance, which has emphasized issuance of cards rather than the full use of the cards' capabilities. As a result, agencies are acquiring and issuing costly PIV cards without using the advanced capabilities that are critical to achieving the objectives of HSPD-12. Until OMB provides additional leadership by guiding agencies to perform the planning and assessments that will enable them to fully use the advanced capabilities of these cards, agencies will likely continue to make limited progress in using the cards to improve security over federal facilities and systems.

Regarding security clearances, in June 2005, OMB took responsibility for a leadership role for improving the government-wide personnel security clearance process. The current interagency security clearance process reform team represents a positive step to address past impediments and manage security clearance reform efforts. Although the President has called for a reform proposal to be provided no later than April 30, 2008, much remains to be done before a new system can be implemented.

Mr. Chairman and members of the subcommittee, this concludes our statement. We would be happy to respond to any questions that you or members of the subcommittee may have at this time.

Contacts and Acknowledgements

If you have any questions on matters discussed in this testimony, please contact Linda D. Koontz at (202) 512-6240 or Brenda S. Farrell at (202) 512-3604 or by e-mail at koontzl@gao.gov or farrellb@gao.gov. Other key contributors to this testimony include John de Ferrari (Assistant Director), Neil Doherty, Nancy Glover, James P. Klein, Rebecca Lapaze, Emily Longcore, James MacAulay, David Moser and Shannin O'Neill.

(311115)

Mr. TOWNS. Thank you very much.
Mr. Sade.

STATEMENT OF MICHAEL SADE

Mr. SADE. Good afternoon, Chairman Towns and Ranking Member Bilbray. Thank you for the opportunity to participate on today's panel to discuss GSA's initiatives implementing HSPD–12, including the establishment of Government-wide standards for secure, reliable forms of identification for Federal Government employees and contractors.

I am pleased to report that, working with our agency customers, we have successfully deployed a complex set of technologies in credential issuing. We have packaged these technologies in an effective and cost-efficient manner to provide agencies with solutions they need at prices they can afford with a business model that is sustainable into the future.

To facilitate Government-wide implementation of the Presidential directive and the requirements that all HSPD–12 implementations be interoperable, GSA took a lead role for the Government-wide implementation. As an initial step, GSA began to dialog with Federal agencies that were faced with the technical, operational, funding, and schedule challenges to meet HSPD–12 requirements.

Next, we established the U.S. access program to offer Federal agencies a compelling solution to meet these challenges. Through the U.S. access program, GSA offers participating agencies a managed shared-service solution that simplifies the process of procuring and maintaining the PIV compliant credentials, while at the same time meeting the demanding HSPD–12 milestones for credential issuing.

The program provides a common infrastructure that is shared by all participating agencies. This allows the cost of building and managing this complex infrastructure to be shared, rather than having each agency attempt to build separate redundant systems on their own.

GSA also provides the project acquisition and financial management support necessary to help participating agencies receive the U.S. access service.

Since launch of the program in 2006, the U.S. access program has enrolled approximately 70 Federal agencies representing the potential to issue between 850,000 to 1 million cards to Government employees. This program serves as an example of how infrastructure and program management expenses can be shared across agency participants to provide overall cost savings for the Government, while improving service quality and decreasing implementation risk.

Specifically agency benefits include centralized program management, which alleviates Federal agencies from having to manage their own in-house HSPD–12 compliant products, built-in HSPD–12 policy compliance. GSA has evaluated the technology to ensure it meets HSPD–12 requirements. Reduce capital expenditures—using a shared service model, the U.S. access program has adopted a simplified, per-credential fee system that eliminates the large upfront cost typically encountered with implementing new informa-

tion technology infrastructures. And, finally, enhanced security. Federal agencies can trust the credentials issued under the U.S. access program by GSA.

There are currently more than 57 U.S. access program enrollment centers located in more than a dozen States, with the majority being in the D.C. area. Ultimately, there will be 225 enrollment centers across the country, 25 of which will be mobile.

GSA additionally sponsors a Government-wide HSPD–12 forum for coordination of implementation activities, common issue resolution, and direction through the Federal Identity Credentialing Committee.

In summary, GSA has created an innovative, full-service program to assist agency customers in meeting HSPD–12 requirements and schedule milestones. Significant progress has been made to deliver cost-effective agency solutions to all HSPD–12 challenges and to develop a sustainable business model.

I thank you for the opportunity to testify today, and I am happy to answer any questions you may have.

[The prepared statement of Mr. Sade follows:]

STATEMENT OF

MICHAEL SADE

ACTING DEPUTY ASSISTANT COMMISSIONER

INTEGTRATED TECHNOLOGY SERVICE

FEDERAL ACQUISITION SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

U.S. HOUSE OF REPRESENTATIVES

APRIL 9, 2008

Good afternoon Chairman Towns and Ranking Member Bilbray. I am Michael Sade, Acting Deputy Assistant Commissioner for Integrated Technology Service within the Federal Acquisition Service within the General Services Administration (GSA). Thank you for the opportunity to participate on today's panel to discuss the current implementation status of Homeland Security Presidential Directive 12 (HSPD-12).

As part of the implementation strategy for HSPD-12, the Office of Management and Budget (OMB) designated GSA to serve three key roles to facilitate the Government-wide implementation of HSPD-12:

1. "Executive Agent for Acquisition of Information Technology" for the implementation of HSPD-12;
2. "HSPD-12 Shared Service Provider" to provide shared HSPD-12 services and infrastructure to Federal agencies; and,
3. Leadership of the Federal Identity Credentialing Committee.

I will describe these three roles and their status in my testimony today.

HSPD-12, signed by the President in August 2004, established the requirements for a common identification standard and credentials to be issued by Federal agencies to Federal employees and contractors to gain physical access to Federal facilities and logical access to systems and networks. The Presidential Directive required four control objectives be met; specifically, that the new identification standard and credentials must be:

1. Issued based on strong criteria for the verification of an individual's identity;
2. Strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
3. Capable of being authenticated electronically; and,
4. Issued only by providers whose reliability has been established by an official accreditation process.

Significant strides have been made to deploy a very complex set of technologies for HSPD-12 credentials in an effective and cost efficient manner that is sustainable into the future. The Department of Commerce was directed by the Presidential Directive to create standards and requirements for the security and interoperability of the credentials and processes required for the Government-wide implementation of HSPD-12. Accordingly, NIST issued Federal Information Processing Standard (FIPS) 201, The Personal Identity Verification Standard, in February 2005. NIST has issued additional technical specifications to ensure that the cards, data stored on the cards, and data interfaces are standardized across Government implementations.

Compliant credentials are referred to as Personal Identity Verification (PIV) cards and must meet the following FIPS 201 requirements:

- PIV cards are "smart" cards that will contain at least one integrated circuit chip for data storage and computational functions;
- Physical printing of PIV cards will provide for standard appearance, mandatory printed information includes: color picture, name, employee and organizational affiliation, card expiration date, card serial number and issuer identification, other data fields are optional;
- PIV card integrated circuit chips will possess the capability to perform data exchange interfaces in both contact and contactless modes;
- PIV cards must contain the following digital credentials: Personal Identification Number (PIN), cardholder unique identifier (CHUID -- a unique number assigned to the specific card, similar to a credit or debit card number), two fingerprint biometric templates, and PIV cryptographic authentication credential (asymmetric key pair and corresponding PIV authentication certificate); and,
- For security and privacy protection, all PIV data stored on the integrated circuit chip will be accessed by contact interface only following card activation through successful PIN entry; the only PIV data permitted for contactless interface is the cardholder unique identifier (CHUID).

Executive Agent for the Acquisition of Information Technology

To facilitate Government-wide implementation of the Presidential Directive and the requirement that all HSPD-12 implementations be interoperable, GSA was designated as the "Executive Agent for Acquisition of Information Technology" for the Government-wide implementation of HSPD-12. GSA established the FIPS 201 Evaluation Program in May 2006 to evaluate commercial products and services for conformance to the normative requirements of FIPS 201. With NIST, GSA has established 23 categories of products (e.g., smart cards, card readers, fingerprint scanners, facial image capture equipment, card printing equipment, etc.) that require evaluation and testing for conformance to FIPS 201 requirements. Commercial industry has responded to the FIPS 201 requirements quickly and effectively; there are now more than 350 compliant products approved for Government-wide use for the implementation of HSPD-12. GSA established an amendment to the Federal Acquisition Regulation to require Federal agencies to acquire only approved products from the FIPS 201 Approved Product List for the implementation of HSPD-12. In this way GSA ensures that the products used for implementation meet FIPS 201 requirements and can, in fact, be interoperable across Government. GSA publicly posts all approved products on the FIPS 201 Approved Products List at our website: www.idmanagement.gov.

HSPD-12 Shared Service Provider

Federal agencies have been faced with very real challenges – technical, logistic and funding – in order to meet all HSPD-12 requirements and aggressive implementation milestones. GSA established the USAccess Program to offer Federal agencies a compelling solution to this challenge. Through the USAccess

Program, GSA offers participating agencies a managed, shared service solution that simplifies the process of procuring and maintaining PIV compliant credentials, while at the same time, meeting HSPD-12 milestones for issuing the credentials. GSA's Managed Service Offering (MSO) is responsible for administering and coordinating the USAccess Program. The USAccess Program provides shared infrastructure and end-to-end services for all participating agencies and allows the Federal Government to leverage the costs to build and manage complex infrastructure, rather than each agency attempting to build separate redundant systems on their own. It provides the project, acquisition, and financial management necessary to help participating agencies receive the USAccess service.

Since the launch of the program in 2006, the USAccess Program has enrolled approximately 70 Federal agencies into the program, representing the potential to issue between 850,000 to 1 million cards to Government employees. The program also serves as one of the Federal Government's best examples of a cross-Government service (i.e. "shared service") where cost, infrastructure and program management expenses are shared across program participants to produce overall cost savings for the Government.

GSA pursued the managed services strategy to save money, but also to improve service quality and decrease implementation risk. Benefits include:

- Centralized program management: Participation in the program alleviates Federal agencies from having to manage the complexities of building and maintaining their own in-house HSPD-12 compliant products. GSA's MSO will manage the acquisition of services, coordinate integration with Government systems, as well as manage contractors for the USAccess program.
- Built-in HSPD-12 Policy Compliance: As the executive agent for the program, GSA has evaluated the technology powering the USAccess system to ensure it meets HSPD-12 requirements. Participating agencies gain immediate access to an end-to-end service that enables them to begin issuing PIV-compliant credentials according to Government milestones.
- Reduced capital expenditures: Using a shared services model, the USAccess program has adopted a simplified, per-credential fee system that eliminates the large upfront costs typically encountered with implementing new IT infrastructures. By leveraging the collective buying power of the Federal Government, the USAccess program spreads infrastructure costs among all USAccess program participants, which in turn reduces the overall price for each individual agency.
- Enhanced Security: Federal agencies can trust the credentials issued under the USAccess program as each credential is registered and verified

according to the requirements outlined by NIST and GSA. By utilizing a standard credentialing system such as the USAccess program, agencies will enhance security and reduce identity fraud. Participating agencies can easily use the USAccess service to procure credentials for their employees and contractors across the United States.

By issuing a common, standard credential to every Federal employee and contractor, the USAccess Program improves Government security and the safety of its citizens. USAccess cardholders can easily identify themselves to other Federal Government workers, while also trusting the identity of other USAccess card holders. At the same time, these card holders will also use their cards to access Government systems and facilities that are critical to performing their jobs. In turn, the Federal Government is able to protect its enterprise infrastructure by validating the identity of people accessing it.

There are currently more than 64 USAccess Program enrollment centers located in more than a dozen states with the majority in the Washington, DC area. Ultimately there will be more than 225 enrollment stations deployed across the country. These are often shared by multiple agencies.

Leadership of the Federal Identity Credentialing Committee

GSA also provides the Government-wide forum for coordination of implementation activities, common issue resolution, and direction through the Federal Identity Credentialing Committee (FICC). All agencies are represented on the FICC to provide a focal point for implementation of the Government-wide identity credentialing capability as required by HSPD-12 and defined in FIPS 201. Members of the FICC are expected to both participate in the implementation of FIPS 201 and champion these activities at the agencies they represent. FICC working groups are tasked with specific work activities to assist in building key aspects of the Government-wide infrastructure for HSPD-12 implementation. A key aspect of this work has been through the FICC Architecture Work Group that has issued the HSPD-12 architecture and technical interface specifications in order to accomplish the long-term objective of Government-wide interoperability of all HSPD-12 solutions.

In summary, the implementation of HSPD-12 has seen major efforts and contributions from industry and Federal agencies and has produced notable accomplishments for Government and industry. The infrastructure that GSA has established for HSPD-12 is critical to meet the requirements of the Presidential Directive and critical implementation milestones. Significant progress has been made in a relatively short amount of time without compromising on the goals of the program and with serious consideration on how to achieve cost-effective implementation.

Mr. TOWNS. Thank you very much.
Mr. Wiesner.

STATEMENT OF THOMAS WIESNER

Mr. WIESNER. Good afternoon, Mr. Chairman and members of the subcommittee. Thank you for inviting me here today to discuss the Department of Labor's HSPD–12 program. We share a common interest in protecting employees, facilities, and information systems.

As reported in our March report to OMB, we have issued PIV cards to over 10,000 of the 15,000 employees at DOL. We have issued PIV cards to over 1,200 of the 2,400 contractors. Overall, DOL has completed PIV card issuance to 66 percent of employees and contractors.

Consistent with the Department's implementation plan, enrollment and issuance of PIV cards continue. Our strategy leverages mobile deployment using DOL resources and what we refer to as a travelers program. This program was established to allow eligible employees, when on official travel, to obtain a PIV card from one of our existing issuing sites located around the country.

As required, PIV cards are issued upon fingerprint results and the initiative of background investigations. To date, 90 percent of our employees have an adjudicated investigation, along with 35 percent of our contractors. We are working toward completion of all adjudicated investigations by the October 2008 milestone.

The Department's efforts to date are derived from the Presidential Directive and OMB guidance. The Department has also complied with OMB's guidance relative to products and services for use in implementing PIV; that is, vendors and components used by the Department are in conformance with the applicable NIST specifications and approval by the GSA evaluation program office.

To meet the first phase of PIV compliance, planning began in late 2004 to establish requirements for a Federal personnel identification system that meets the control and security objectives of the directive. A certified process was completed and approved in October 2005.

To meet the second part of the PIV compliance, the Department, consistent with our internal information technology governance, developed the program as an IT investment. In early fiscal year 2006 the Department conducted a performance analysis of our legacy badge system to identify functionality and technical gaps between this system and the PIV II requirements. As a result, the system was identified as not compliant with FIPS 201 requirements.

Without a PIV II compliance solution that would meet the mandated security and technology guidelines, the Department conducted market research to identify viable alternatives to comply with HSPD–12 requirements. Potential alternatives included relying exclusively on shared services offered by the GSA or the Department of Interior, Department of Labor-owned IT solutions to cover all Federal and contractor employees throughout the country, or a hybrid model that utilized a Labor-owned IT solution to conduct PIV card activities in facilities with high concentrations of employees, while using a shared service for facilities with small em-

ployee populations, where deployment of IT infrastructure would be cost prohibitive.

In the absence of an existing DOL IT solution for identity management, and at the time the emerging status of constraints and schedule capabilities and unknown costs associated with a shared service solution, the Department in April 2006 decided to move forward with the hybrid option of the Labor-owned IT solution, with plans to use GSA shared services as they became widely available.

Later this year, DOL plans to utilize GSA shared service sites for our employees who are yet to be issued a PIV card, particularly remote locations with small DOL populations.

The Department is already leveraging the PIV card in our Boston and New York regions, where regional staff worked with the GSA to use the DOL PIV card for physical access control.

In addition, the Department has initiated planning activities associated with the deployment of the physical access control system at DOL headquarters. Our plans are to begin with a pilot of this technology at one facility in Washington, DC, later this year. Simultaneously, in fiscal year 2009, we will begin planning activities associated with the use of PIV cards for access to information systems through the deployment of logical access control system technology.

To date, the deployment of HSPD–12 solution has enabled the Department to streamline and tighten the processes associated with identity verification and PIV card issuance. The Department's goal is to extract the full potential benefits of this HSPD–12 investment.

In conclusion, the HSPD–12 program is a core element of our business and operational culture at the Department of Labor. Secretary Chao, Chief Information Officer Pizzella, agency senior management, and our dedicated employees are committed to the success of the Department's HSPD–12 program.

Mr. Chairman, thank you for the opportunity to provide a brief outline of the Department of Labor's approach to HSPD–12. I would be happy to answer any questions.

[The prepared statement of Mr. Wiesner follows:]

STATEMENT OF THOMAS C. WIESNER
DEPUTY CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF LABOR

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

APRIL 9, 2008

Good afternoon, Chairman Towns, Ranking Member Bilbray, and Members of the Committee. Thank you for inviting me here today to discuss the Department of Labor's (DOL) implementation of the Homeland Security Presidential Directive (HSPD)-12 program, our plans for meeting the Office of Management and Budget (OMB) deadlines, and the means by which the full capacity of the new standards will be applied within the Department. We share a common interest in protecting employees, facilities, and systems.

Today, I will first speak on the background and success of implementing and adopting the Personal Identity Verification standards I and II (PIV-I and PIV-II) at DOL, as it relates to OMB deadlines. I will then expand on the current status of the Department to leverage the credentials on the PIV card to further secure the Department's facilities and access to information systems, as well as the benefits this program has brought to the Department as a whole.

1. Summary of DOL's HSPD-12 Efforts

As of the Department's March report to OMB, we have issued PIV cards to 10,591 of the 15,407 employees at DOL (69%). We have issued PIV cards to 1,210 of the 2,400 contractors (over 50%). PIV card issuance is consistent with the process guidelines contained in Federal Information Processing Standards (FIPS) 201. DOL is on track to reach implementation goals reported to the OMB in our "December 20, 2007 HSPD-12 Implementation Plan Update." Overall, DOL has completed PIV card issuance to 66% of employees and contractors.

Consistent with the Department's plans to meet the October 27, 2008 OMB deadline, enrollment and issuance of PIV cards continue. DOL's strategy leverages mobile deployment using DOL resources and what we refer to as a "Traveler's Plan." This plan was established to allow eligible employees, when on official DOL travel, to obtain a PIV card from one of our existing DOL issuing sites.

As FIPS 201 guidelines require, PIV cards are issued upon fingerprint results and the initiation of background investigations. To date, of DOL's 15,407 employees, 13,827 or 90% have an adjudicated investigation, along with 35% of contractors, bringing the overall completion of adjudicated background investigations to 82% of employees and contractors. We are working towards completion of the remaining 18% as required to meet the October 2008 milestone. The Office of Personnel Management (OPM) was a key partner in DOL's ability to implement an efficient electronic fingerprint submission process. This process was previously paper-based, and turn-around could span several weeks from submission to results. Based on our experience, results now average five to seven business days from date of submission to OPM.

The capabilities of these new DOL-issued PIV cards are already being leveraged at DOL-occupied General Services Administration (GSA) facilities in New York and Boston. In partnership with GSA, DOL has demonstrated the value of the PIV card technology by eliminating the need for employees to have two cards; a GSA-issued PIV card for facility access, and a DOL-issued PIV card for visual identification. Beginning in FY 2009, DOL plans to begin projects, which use the PIV card for logical access to government information systems.

2. Background

The Department's HSPD-12 efforts to date are derived from the Homeland Security Presidential Directive (HSPD) -12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive), signed by the President on August 27, 2004. The Directive requires development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. The high-level goals of the Directive are to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy.

As required by the Directive, the Department of Commerce issued FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors." Additionally, the Department complied with OMB memorandum M-05-24 "Implementation of Homeland Security Presidential Directive-12 – Policy for a Common Identification Standard for Federal Employees and Contractors." Memorandum M-05-24 provides the phasing-in of PIV standards. OMB mandated milestones spanned from October 27, 2005 through October 27, 2008, and comprised two major PIV goals: PIV-I by October 27, 2005, and PIV-II by October 27, 2006.

The Department has also complied with OMB's guidance relative to products and services for use in implementing PIV. Vendors and components used by DOL required conformance with the applicable Department of Commerce and NIST standards and guidelines along with testing and approval by the GSA FIPS 201 Evaluation program office.

PIV-I Compliance

Planning to meet PIV-I objectives began in late 2004. The objectives were to establish requirements for a Federal personal identification system that meets the control and security objectives of the Directive, including the personal identity proofing, registration, and issuance process for employees and contractors. A certified process was established and approved by the Agency's Designated Approving Authority. Throughout the planning and execution phases, DOL leveraged the input and buy-in from key operational stakeholders, as it became evident that collaboration among the Human Resources, Security, and Information Technology (IT) functional areas would be necessary for the implementation of a successful HSPD-12 program.

In October of 2005, the Department met OMB M-05-24 requirements for compliance with FIPS 201 Part 1, which satisfied the objectives and met the security requirements of HSPD-12.

PIV-II Compliance

The Department began planning activities in the fall of 2005 for the PIV-II phase of the project, which focused on meeting the technical interoperability requirements of the Directive.

To effectively manage the Department's IT development and maintenance efforts associated with the deployment of a compliant HSPD-12 PIV-II solution, the Department, consistent with internal information technology governance, developed the program as an IT investment. This means all phases of the DOL *IT Capital Planning and Investment Control Management* life cycle apply to the management of the project.

The Department also conducted a performance analysis of the legacy badging system, to identify functionality and technical gaps between this system and the new PIV-II process and requirements. As a result, the system was identified as non-compliant with FIPS 201 requirements.

Without a PIV-II compliant Identity and Access Management Solution or infrastructure that would meet the PIV mandated security and technology guidelines, the Department conducted market research to identify viable alternatives to simultaneously close the performance gaps and comply with HSPD-12 and its derivative requirements.

Potential alternatives ranged from:

- Relying exclusively on the shared services offered by the GSA or the Department of Interior.

- Deployment of DOL-owned IT infrastructure to cover all federal and contractor employees throughout the country; or

- A hybrid model that utilized DOL-owned infrastructure to conduct PIV card activities in facilities with high concentrations of DOL resources, while using a shared service for facilities with small DOL populations, where deployment of DOL-owned infrastructure would be cost prohibitive.

Decision to Implement the Program Independently

In the absence of existing DOL infrastructure for identity management, and the emerging status of constraints in schedule, capabilities, and at the time unknown costs associated with a shared service solution – from either the GSA or Department of the Interior - the Department, in April 2006, decided to move forward with the hybrid option deployment of a DOL-owned infrastructure with plans to use GSA shared services as they became widely available. This approach would allow us to meet the October 2006 OMB goal. Just as important, it would also establish the foundation for the Department's Enterprise-wide Identity and Access Management framework. After the decision was made, DOL submitted this updated HSPD-12 Implementation Plan to OMB in September 2006.

3. Current Status

In accordance with OMB guidance, DOL has posted quarterly status reports for the program since March 1, 2007, with details on the number of PIV cards issued to both federal employees and contractors. Additionally, the Department has provided required updates of its implementation plan to OMB. The last submission was on December 20, 2007. This update addressed how DOL will optimally meet the remaining OMB milestones.

As a partner with GSA in this ongoing government-wide effort, DOL plans to utilize the GSA shared-service sites close to DOL employees who are yet to be issued a PIV card, particularly remote locations with small DOL populations. We have begun preliminary discussion with the GSA program office to establish use of their PIV services.

Leveraging the PIV Cards for Physical and Logical Access

The Department is already leveraging the PIV card in the Boston/New York Region, where DOL regional staff worked with the GSA to prepare for and allow use of the DOL PIV card for access control at the New York Varick Street and Boston JFK Building locations. The GSA Boston location takes advantage of the advanced security features of the DOL PIV card for electronic authentication. In order to further maximize the value of the new PIV card for identity authentication and validation, the Department has initiated planning activities associated with the deployment of a PIV-II compliant Physical Access Control System (PACS) at DOL Headquarters. Our plans are for this to begin with a pilot of PACS technology at one DOL facility in the Washington, DC area. Simultaneously in FY 2009, DOL will begin planning activities associated with use of the PIV cards for access to information systems through deployment of logical access control system technology.

4. Benefits Achieved Department-wide as a Result of HSPD-12 to Date

To date, the deployment of the HSPD-12 PIV-II solution has enabled the Department to streamline and tighten the processes associated with identity verification and PIV card issuance for both employees and contractors.

In order to comply with FIPS 201, the Department has worked diligently to close any gaps associated with background investigations for DOL employees. Background investigations are now a part of the streamlined PIV process and are a prerequisite for the PIV system, prior to PIV card issuance. This integration has resulted in increased and timely completion of background investigations. The collaboration between DOL and OPM is instrumental in this success.

We are confident that we will continue to meet HSPD-12 milestones as outlined in our implementation plan to OMB. The Department's goal is to extract the full potential HSPD-12 benefits of this investment in PIV.

In conclusion, the HSPD-12 program is a core element of our business and operational culture at the Department of Labor. Secretary Chao, Chief Information Officer Pizzella, agency senior management, and the dedicated DOL employees are committed to the success of the Department's HSPD-12 Program.

Mr. Chairman, thank you for the opportunity to provide a brief outline of DOL's approach to HSPD-12. I would be happy to answer any questions.

Mr. TOWNS. Thank you very much. Thank you all very much.

Let me start out with you, Ms. Koontz. Do you think the Federal Government buildings an information systems are more secure today as a result of HSPD–12?

Ms. KOONTZ. Mr. Chairman, I think we have to say that there has been a marginal improvement in security. One of the aspects of the new standard is to provide for a uniform way of doing background checks on all Federal employees before credentials are issued, and this is being implemented by all Federal agencies, and they have, in fact, completed most of the background investigations as of this point in time, so I think that is something that does increase security.

To the extent that agencies are using any of the electronic capabilities in the cards, that is an improvement; however, we have to point out that the majority of agencies are not yet in the position to use the electronic authentication capabilities in the cards, so in those cases what we have is a large outlay for expensive cards, and we are not receiving associated and corresponding benefits to security.

Mr. TOWNS. So let me put it this way. What has been wasted? Have you assessed that?

Ms. KOONTZ. I could not give you a number to quantify what that was, but I think to some extent how the system was implemented has been wasteful. In any case where cards have been issued and the cards, I think someone said before, cost $82 for the first year, $36 per year for the next 4 years, for over a life of 5 years. When those are issued with that kind of outlay but they are still being used just for visual inspection, there is really no increase in security benefits.

What we recommended is that we wanted to see more emphasis on putting together the security systems that will make the cards be able to be used, and also to align the acquisition of the cards with the ability to be able to optimize their use.

Mr. TOWNS. Thank you.

Ms. Evans, GAO says that because OMB directs agencies to distribute the new ID cards to employees according to a set time line, but does not also direct them to get the readers and equipment to use them, that money and resources dedicated to HSPD–12 implementations are actually being wasted.

Ms. EVANS. Sir, if we could step back, first and foremost about the money that is being wasted I think we should really look to see how many cards have actually been issued. It is 3 percent. So it is 180,000 credentials out of the potential 2.5 million for the Federal employees that we have to do. So I would actually say that we have been very mindful of the taxpayers' dollars going forward.

What the program has really been focused on, and so this is why we should step back from card readers and really look at what HSPD–12 was intended to do. It is building off of existing programs that were already there. We had a program out in place that was looking at all of the IT investments, which we called e-authentication. We issued guidance back in 2003 for agencies to look at their IT systems, their physical access systems, all those types of things and assign a level of security risk associated with that.

HSPD–12 builds off of that, but what is really important about HSPD–12 is getting a common business practice so that when Department of Commerce issues a credential, that DOD has trust in that credential; that they know that they have used the same business processes, that they validated that individual or that contract in the same way, that contractor in the same way, so that they can trust it.

So what we have been really very focused on is the foundation across the Government, having agencies really look at what are those positions, who are those contractors, who is coming into your facility, should they even have access to your facilities, should they have access to your IT systems. That takes a lot of work for the agencies to really go back, look at that, and then fully vet those people in a standardized way so that once that credential is issued, if you as an agency then say, OK, Contractor A who is under a contract over at Commerce, now they are a contractor over here at DOD, I need to have them come into my facility. I need to have them access my systems. You can trust that credential. And then the level of trust that you are using, you know that you can start using these other features.

But what is critical here is getting the foundation and those business processes normalized and harmonized across the Government so you can trust it.

Mr. TOWNS. Thank you.

I guess my real question is why hasn't OMB mandated the purchase for readers and scanners?

Ms. EVANS. Because every agency needs to go back. We have implementation plans of this. They are building this into the regular life cycle of their investments. Agencies have to look to see is that really what is necessary for each and every facility and have a full comprehensive plan. They are going to be doing that on a different time line.

We put into policy the target date of the critical activities that we thought that they needed to have across the board in all agencies, but it varies. The implementation plan is going to vary, because what Department of Interior needs to have, you may issue identification cards for people that are out in the field but you don't have to have card readers going into Yosemite National Park.

So what we are doing is working with each individual agency, having them analyze the risk, look at what they really need. Where do they need to have card readers? Is it appropriate to have the card reader? And then make sure that there is a program in place so that they can buy them and implement them in a very efficient way, which is what GSA has outlined.

Mr. TOWNS. Let's hear from GAO on this.

Ms. KOONTZ. Where to begin. It is true that Ms. Evans is correct, there have been few cards issued to date because none of the agencies meet the deadline for issuance. I think that is actually, in some ways, fortunate, because I think we have an opportunity to make a mid-course correction before we go on and issue new cards without being able to fully exploit their capabilities, so I look at that as an opportunity to get things back on course, and that is exactly what we recommended in our report.

The whole issue of building the underlying security systems that allow you to use the electronic capabilities of the card, I think that is the foundation that we are talking about. Ms. Evans talked about needing the foundation, and I think that is the foundation that we have to work on, and we have to have goals for implementing that foundation, and we need to put more emphasis on that, rather than just emphasizing the issuance of cards, especially in cases where we are not ready to use the electronic capabilities.

It may be true that a card reader may not be needed in Yosemite. I am not sure. But in the vast majority of cases you are going to want to use some kind of electronic authentication. You are going to want to read that card in order to authenticate the individual's identity, and you are also probably going to want to have some kind of visual inspection so that you have a couple factors of identification to make sure that yes, that is the person that they claim to be, and that card is authentic.

Mr. TOWNS. Don't you think it is important to set some goals or mandates or do something? I figured you will come back here 2 years from now or 3 years from now and still be at this level.

Ms. KOONTZ. I think what you see here is the power of goals and mandates. When OMB says what we are going to be tracking over time is the number of background investigations that we are doing and the number of cards that were issued, that is going to be the focus for Federal agencies, because that is what has been set out to them as the priorities.

I think what we are asking for is to add other goals that have to do with establishing the foundation to best use of cards.

Mr. TOWNS. I yield to the ranking member, Mr. Bilbray.

Mr. BILBRAY. Thank you.

Karen, the evaluation was kind of disappointing. What is your reaction to it?

Ms. EVANS. As far as GAO's report, we use the reporting overall, and we recognize the power of setting targets and milestones, so I agree with both what you guys are saying. I am not necessarily disappointed that the credentials weren't issued, because we recognize that there were issues associated with that, and that is why we came out with additional guidance working with the agencies on what the problems were. We were using that information.

There were several challenges going forward with this program. First and foremost, what we wanted to do, the technology didn't exist, and so industry rose up to that. NIST, in setting the standard, did it in less than 6 months, so this is a very aggressive program, but when you put it in the frame of implementing the recommendations of the 9/11 Commission it really falls behind the mark of improving the security.

So I am disappointed from the aspect that we aren't further along, just like you are, but what we do believe we have done is made it a more comprehensive program, so when we talk about card readers and looking, you are only looking at one piece, which is physical access. We are also using this card for logical access, which is information security and system access. So that is where we have done a lot of making sure that the milestones are there. We issued additional guidance after the VA situation. We said that

agencies had to use two-factor authentication. This card allows for that two-factor——

Mr. BILBRAY. Two-factor identification?

Ms. EVANS. Yes.

Mr. BILBRAY. What is that?

Ms. EVANS. So the idea of two-factor identification is something you have and something you know, so a password is something you know, the card would be something you have. You use the two of those in conjunction to make sure that the person who is getting on the system is the person who it should be.

Mr. BILBRAY. Ms. Dillaman, the backlog concerns, are you able to use biometrics in your background checks?

Ms. DILLAMAN. Yes, sir. Every background investigation includes a biometric check of the FBI's record. So to the extent that there is a biometric name base search conducted, that is universally applied across Government.

Mr. BILBRAY. You get into the FBI files, just like most law enforcement. Can you go into the INS files?

Ms. DILLAMAN. Biometrically, no.

Mr. BILBRAY. Why not?

Ms. DILLAMAN. We have no biometric exchange system in INS.

Mr. BILBRAY. Mr. Chairman, every immigrant coming into this country is now being biometrically read. Every immigrant legally entering into the country is put into the system. Every illegal immigrant who is detained is put into the system. Now we have a background check that can't access those codes.

I am concerned that these kind of firewalls—and I am not blaming you for it, I just think that one of the things that we need to talk about is the fact that we have a data base system over there. And it is not just you, it is local and State law enforcement, too, that we have these firewalls that were developed after the Watergate fiasco so that now we are still out there, and I am just concerned about the ability. I think anybody would say it is reasonable that you should be able to have access to all the Federal records that may be able to detect that somebody coming in under one name is not exactly what they say.

Ms. DILLAMAN. And perhaps maybe I can alleviate some of those concerns, because we are working with Homeland Security and the FBI, tying those three systems together, so that INS' records of concern are available to us through that biometric search that we send to the FBI. Every fingerprint that I receive, whether I receive it electronically or hard copy, if I get a hard copy I immediately convert it to a digital image, which allows me to move that around system to system. I transmit the image to the FBI, and the FBI can cross-reference that with INS' records.

I think we are on the cusp of being exactly where you would like us to go.

Mr. BILBRAY. I am trying to make a point that the D.C. snipers, if the one immigrant had not committed a misdemeanor, even though we had the fingerprints at a murder site, law enforcement would not have been able to know about this except for the fact there was a misdemeanor and so the record was transferred out of INS' records over to FBI to where then the Alabama officials were able to detect it. That just shows you how close we were not to

catching this guy. Thank God he committed the misdemeanor so that we could stop the killing spree.

That is a major concern of mine, but we are using the biometric fingerprinting system as first sweep right across the board, right?

Ms. DILLAMAN. Absolutely.

Mr. BILBRAY. And now when we are going in with implementation of real IDs, States are now going into a data bank based on all the new drivers' licenses, too?

Ms. DILLAMAN. Yes.

Mr. BILBRAY. OK. Thank you very much. I appreciate it.

Thank you, Mr. Chairman.

Mr. TOWNS. Thank you.

Ms. Dillaman, we hear from OPM that the security clearance backlog has been eliminated and the OPM has exceeded the requirements of the 2004 intelligence reform law, but Federal agencies and entities say they still have a serious problem with backlog and delays from OPM, and they are very skeptical of your claims that the backlogs are gone. Can you be very precise in explaining what you mean when you say there is no backlog?

Ms. DILLAMAN. Certainly, sir. We track every investigation, and every single hand-to-hand process with that, so my data is hard and accurate, and we have been measuring every investigation, beginning to end, with those types of metrics.

The best way I can demonstrate the backlog elimination was 7 years ago, when we merged the program with Defense Security Service's program there was a pending backlog investigations inventory of over 700,000 investigations. We do 2 million a year, the combined organizations. The 700,000 was over twice what it should have been if you were processing cases timely and current.

Today our inventory is around 285,000 total investigations of all types—national security, public trust, and basic suitability investigations.

The percentages I gave you, mid-60 percent of all initial national security investigations averaged in the mid-60 days. That was 80 percent, I am sorry, in 60 days. These are hard and fast numbers.

Anecdotally, are there investigations that take much longer? You bet. There are investigations that probably should take a while because there are issues developed that we had to explore. We have problems accessing third-party information, but 145,000 people had the initial clearance investigations done in under 45 days last year, too. It is usually the ones that are delayed that are getting the most attention. But by pulling enough resources, Federal and contractor combined, dedicated to the background investigations program, working to improve access to the information critical to the process—and it is building electronic bridges between us and Federal agencies, all 50 States, and over 20,000 local law enforcement agencies. By getting our automation systems, we have been able to do that.

I think it took a long time for everyone to identify just how bad it got in the year 2000, and it has taken a long time to notice this improvement, as well. But that is where we are at today. There is no backlog because of insufficient resources.

Mr. TOWNS. Let me ask you, Ms. Farrell, if you have any thoughts on that issue. I know you did a lot of work with this.

Ms. FARRELL. Certainly. GAO has done a lot of work in this area over the last three decades, and the backlog that Ms. Dillaman is referring to, GAO reported in 2004 about the fact that DOD did not at that time even know what the backlog was. We went in and we calculated it with help from the agencies and made recommendations regarding how DOD could get control of the backlog, and suggested that they had a plan to move forward.

There have been a number of positive steps, as my colleague noted in her opening statement, in terms of what the agencies have done, including OPM and OMB, in trying to manage the backlog. The question here is what is your definition of a backlog. We have not looked at that for a couple of years. We have started work in February to go in and look at the timeliness and the quality of investigations and adjudications for the DOD program, as well as we will be starting up work looking at the Intelligence Committee. But our understanding is that OPM, when they look at the backlog, they are looking at investigations that have been done in 180 days versus the Intelligence Reform and Terrorism Prevent Act that requires that investigations, as she has noted, be done within 90 days for the investigation part. So I think there is still a great deal of work to be done in the area of the backlog.

But, again, we don't have hard and fast data. We are in the middle of looking at that to see what is the backlog, not just for investigations but adjudications, as well.

Mr. TOWNS. We have heard the need for reciprocal clearances. If I receive a security clearance in order to work for one agency, that clearance ought to be good enough for another agency, especially because the guidelines for adjudication come from the administration. Why are agencies still being allowed to refuse to recognize each other's clearances? Why?

Ms. FARRELL. Do you want me to take that? We think it may be because of the quality, the quality of the investigations. There are Federal guidelines that the adjudicators, as well as the investigators, are supposed to adhere to, but the metric that has been missing for all six phases of the clearance process is quality metrics. OPM has reported for one of the six phases that for the investigative phase that they do look at the number of investigations that are returned because they are incomplete, and they count that as one of the metrics, but we think that there are a number of metrics that should be used from the time that DOD or the other agencies determine the requirements, as well as the application submission process, the investigation process, the adjudication process, the appeal process, and if there is a need to reopen the case.

Again, there are six phases of the clearance process, and there are not metrics for all six to determine the quality. Thus, the reluctance, I think, of some agencies to accept a clearance from another one, not knowing which standards have been adhered to.

Ms. DILLAMAN. If I may, I think there is also some confusion about reciprocal accepted security clearances and suitability determinations. It is true that a security clearance is reciprocal acceptable. If you obtain the top secret level of one agency, you can and should move seamlessly to another position requiring a top secret clearance.

When it comes to determining basic suitability for a position, however—and Federal civil servants are held to suitability standards—there are some position-specific requirements. Past drug use may not be an issue in some agencies, but it very much may be an issue in DEA. The former Smith Amendment that precluded security clearances in some agencies but not all might have meant that someone could have had a felony conviction with one agency and had a clearance, but have been able to move seamlessly, reciprocally to the Department of Defense.

Now all of those issues are being worked on, including providing transparency into the suitability determinations. So if individuals determined to be suitable for a job but may not be suitable, specific position factors have to be considered. We have to add transparency into that issue, as well.

Mr. TOWNS. Is that because you are using contractors?

Ms. DILLAMAN. No, sir. Not at all. The contractors who are used to do the background investigations are trained and cleared to exactly the same level as their Federal counterparts. They are held accountable to the same standards of performance.

Mr. TOWNS. I just think that some way or another if a person is cleared, I mean, there should be some kind of working relationship here that everybody could sort of respect and accept and move forward on.

Ms. DILLAMAN. And to support that, one of the mechanisms which we do have in place is that if you went to work for the Department of Treasury, for example again, and have a top secret clearance, you then move to Homeland Security and Homeland Security asks for a new investigation, that would be denied. We would reject Homeland Security's request because a sufficient investigation is on file that supports you being reciprocally moved, accepted into another agency.

Mr. TOWNS. Let me move then to you, Mr. Sade. The FIPS 201 card relies mainly on integrated circuit chip for security. This chip stores data and communicates with the card readers. Isn't it true that chip can be imperceptibly destroyed by kinking it with a sharp object, even your fingernail? I would also like to hear also from you, too, on that, Ms. Evans. Is that possible?

Mr. SADE. If the card is left exposed, I believe that is possible, but all the cards are issued with a card holder to protect it.

Ms. EVANS. Well, I mean, I don't have anything other than what you have said. I mean, technically that could happen. You could destroy the card. You could mess up the way the card works. You can do that now on a credit card by putting two magnetic strips together. You can do that on a whole lot of technical cards. I mean, we do take the precaution by making sure that there are protective covers associated with the card so that you can slide them in and out and be able to read them appropriately and put them into card readers, so that can happen, but that can happen on any technical device or any type of card.

Mr. BILBRAY. Mr. Chairman, I want to go home and put all my wife's credit cards together. [Laughter.]

Mr. TOWNS. Good idea.

Mr. BILBRAY. But, I guess, to followup on it, is this very much different than the technology that has been used in the Metro for

over 15 years, and that is the electronic reading capabilities that they had there? Do you know?

Ms. EVANS. It is enhanced. There are several things that are on the card, and that is what is outlined in what we call the FIPS, the Federal Information Processing Standard, so there is a lot more information, but it does have a strip, so it is using something similar but there is a lot more information that is encoded on the card.

Mr. TOWNS. Let me thank you very, very much, of course, for your testimony. I see we still have a long way to go, and of course we have I think the question that I really want to raise: is it the lack of resources? I mean, what else do you see that might be a problem here as to why you are not being able to have more? Is it 3 percent?

Mr. BILBRAY. I mean, you have to worry about why aren't the readers out there, and you say because we only have 3 percent out there. Then the problem isn't that the readers aren't out there; the darned cards aren't out there.

Mr. TOWNS. Yes. So what do you see that needs to be done? Is there anything that needs to be done to sort of help facilitate this?

Mr. BILBRAY. And to back that up, do you want to comment on the GAO's recommendation that you set reasonable limits and have your Departments articulate how they are going to fulfill those goals?

Ms. EVANS. First, on the GAO report, I would say that most agencies would argue that we have set really aggressive dates, and the public would say we set really aggressive dates. I would concur with you that the dates aren't aggressive enough.

However, as far as setting milestones out into the future, again, we are working with the agencies on a case-by-case basis, so where you could help and how we are talking about this is that it is hearings such as this and then going back and asking the agencies about the risk and how they are assessing the risk and what is their overall security posture of what they want within their departments and their agencies.

This is one thing that makes it a little bit more difficult. This is where a Secretary is willing to live with how much risk, and when you know that, then OMB can work and aggressively help that agency achieve that.

We are looking at all of the security initiatives across the board, the information security ones as well as the actual systems. And when I see an agency that doesn't have a good report in from its Inspector General on certification and accreditations related to how they assess risk, I am putting my efforts into how are you doing that, because then I really am going to have the agency waste taxpayers' dollars if they are just trying to be compliant with OMB mandates and hitting milestones.

Mr. BILBRAY. Well, in that GAO report they specifically gave you a vehicle that businesses used all along, and that is a detailed explanation of how you are going to reach your goals, with a specific plan, rather than just having arbitrary numbers, this is our goal, this is how we are going to do it.

Ms. EVANS. We have those.

Mr. BILBRAY. Those plans, in fact, can warn you that maybe you don't have the right goals.

Ms. EVANS. But we do have those plans, and we have the plans for all the security initiatives across the board, and we are looking at those. The GAO report is looking at HSPD–12 in isolation and it is not looking at the security posture of the agency as a whole, looking at the other types of activities and the other guidance that we have put in place, like our data breach guidance that looks at both physical and logical and says, When are you going to have encryption, and when are you going to have the two-factor authentication, and when are you going to meet all of these types of activities. This is a key initiative, and if you are not going to have encryption in place until 2010 and you will have these in place, and then you are not going to be sure who all is in place, we are looking at all of those across the board.

Mr. BILBRAY. I understand that, Ms. Evans, but, to use the analogy I started off this hearing with, that would be like the Army saying you are right, we need more body armor in the field, but we are also looking at now the armored Humvees, and that is something we have to consider when we are talking about the body armor.

The fact is that the crisis, the fact that there has been so little movement done that there needs to be some priorities made here. And this was a very simple one that was laid out not just by the President, but by the men and women that studied the 9/11 situation and said this is our No. 1 Achilles heel in the United States. It doesn't say there wasn't enough cops, enough bombs, enough tanks; it said enough IDs and a secure identification system for this country is absolutely essential.

Ms. EVANS. Sir, I am not disagreeing with you, sir. I agree with you. But it is not the actual card issuance that is the measure of that, it is the business process prior to issuing the card. So OMB is very sensitive to when we establish milestones, that we want to make sure that agencies just aren't complying and doing volume without really achieving the goal of the improved security, as you stated.

Mr. TOWNS. Is this equipment widely available for purchase? I am getting the feeling that something else is going on here. Is it?

Mr. SADE. As I mentioned, we had the shared service model for those 70 agencies that are going through us, and we are still in the process of deploying the 225 enrollment stations. But part of the service we provide, part of the General Services Administration, we have what we call the GSA schedule contract, Schedule 70, which is for information technology. We have gone through, working with NIST, and tested anybody that wants to put their equipment and make it available for sale across the Federal Government, and they put that equipment on their scheduled contract, and we test it before it goes on. I believe Ms. Evans in her testimony mentioned the 300-plus products that are available today on those schedules.

I would also note that those schedules not only are available for use by the Federal Government; they are also for use by State and local. So if State and local governments want to buy complying equipment, it is available to them, as well.

Mr. TOWNS. Let me ask you this, Mr. Wiesner. Several Federal agencies, including the Department of Labor, have opted not to use GSA service for complying with HSPD–12. Labor told our staff they

were not convinced that GSA would be able to meet OMB's deadlines; however, GAO reports that Labor is not in good shape to meet OMB's deadline, either. So is Labor equipped to comply? I just don't know what is going on here.

Mr. WIESNER. Well, we went out on our own. As I said in my testimony, we did not have an identity management system at the Department of Labor prior to HSPD–12. We had a simple data base that issued a dumb badge for Federal employees. We had a hard time managing contractors, etc. You saw the added dollars to build out an identity management infrastructure to pay benefits not only for HSPD–12 for cards, physical access, logical access, but integrated into some future planned initiatives like our H.R. system, so we could make it part of the hiring process as well as the determination process, strengthening our contractors and knowing who our contractors were and who had clearances. So we saw that investment back in April 2006.

We are very serious about meeting the first October goal from OMB which said you have to issue at least one card by October 27, 2006, so we took that very seriously and looked at how we were going to meet that and in April 2006 we had to make a decision to go to shared service provider or build out this infrastructure, and as I mentioned we treated this as an IT investment, looking at the whole benefits of the dollars we were about to spend and made the choice that it was worth the investment to build out our own infrastructure and start issuing cards to meet the OMB mandates in October 2006, as well as the subsequent milestones that have been laid out upon us.

As I also testified then, since GSA has now made readily available many enrollment and issuing stations around the country, perhaps upwards of 15 percent of employees will go to a GSA shared service center.

Mr. TOWNS. What percent?

Mr. WIESNER. About 10 to 15 percent. We are at 60 percent now. We have issued as of early this week over 11,000 badges to our 15,000 employees. We are well over 67, 68 percent. As you go out to the smaller locations, it becomes cost prohibitive for us to do this on our own. That is when we will go to GSA and go through the GSA process and pay the card fees associated with the shared service model. We fully intend to use that model where it makes financial sense, as well as to get to those employees that need a card. We are targeting to be as close to 100 percent as possible by October of this year.

Mr. TOWNS. You have the funding?

Mr. WIESNER. Through fiscal year 2008, yes.

Mr. TOWNS. Let me thank all of your for your testimony. We look forward to working with you to try and move forward. You know, 3 percent is not impressive. I guess you know that. I think my colleague mentioned about three or four times 3 percent. I think that isn't right. That is not acceptable. I think we have to move much more aggressively. Just 3 percent?

Anyway, thank you so much for your testimony. We appreciate the work that you are doing. Thank you.

Our next panel consists of Robert Zivney, vice president, marketing, Hirsch Electronics, representing the Security Industry Association. Welcome.

We also have Mr. Benjamin Romero, Chair of the Information Technology Association of America Security Clearance Reform Task Group, representing the Security Clearance Reform Coalition.

It is a longstanding policy of this committee that we always swear in our witnesses, so will you please stand and raise your right hands?

[Witnesses sworn.]

Mr. TOWNS. Mr. Zivney, you may start. What we do is that we allow the witnesses 5 minutes to sum up, and then we would have a question and answer period after that, so if you could make your statement within 5 minutes, we greatly appreciate it. We have a light that starts out with green and then goes to yellow to let you know that your time is almost up, and then when it comes to red that means your time is up.

You may start.

STATEMENTS OF ROBERT ZIVNEY, VICE PRESIDENT, MARKETING, HIRSCH ELECTRONICS, REPRESENTING THE SECURITY INDUSTRY ASSOCIATION; AND BENJAMIN ROMERO, CHAIR, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA SECURITY CLEARANCE REFORM TASK GROUP, REPRESENTING THE SECURITY CLEARANCE REFORM COALITION

STATEMENT OF ROBERT ZIVNEY

Mr. ZIVNEY. Chairman Towns, Congressman Bilbray, members of the subcommittee, thank you for the opportunity to testify about the implementation of Homeland Security Presidential Directive 12. My name is Rob Zivney. I am the vice president of marketing for Hirsch Electronics, headquartered in Santa Ana, CA. Hirsch Electronics is a manufacturer of physical access control systems for non-residential markets, including the Federal Government.

I am honored to testify today on behalf of the Security Industry Association [SIA], which represents 400 manufacturers, integrators, and dealers of electronic security equipment. SIA members provide solutions for physical security to protect people and property of America in their schools and hospitals, their airports and seaports, their factories and offices, and especially their buildings of government.

SIA members are committed to offering assistance to ensure the successful implementation of this directive in all Federal agencies.

Mr. Chairman, HSPD–12 and the associated standards developed by NIST, specifically the identity vetting process, forms a far stronger foundation for security than we have ever seen.

Routine access transactions are enhanced by the use of the credential bearer's fingerprint templates derived from the same fingerprints used in the background check process. However, SIA believes that cost and time required for implementation of HSPD–12 were underestimated by OMB. Traditionally, the functions of authentication and authorization resided with the administrator of a local physical access control system [PACS].

As a result of HSPD–12 and FIPS 201, the accountability for authentication now resides with the credential issuer, while authorization remains a function of the PACS.

The development of this new shared infrastructure presents a significant learning curve for us all.

Mr. Chairman, implementation of HSPD–12 is a true pioneering effort. It requires those responsible for human resources, information technology, and security to cooperate on an unprecedented level. Although HSPD–12 may not draw the attention of our Nation's major media outlets, the world is watching. In spite of technical and procedural challenges, our own success has attracted the scrutiny of other nations and local governments and private industry.

In our view, an identity credential that uses fingerprints and public key infrastructure [PKI], will revolutionize global standards for security, and promises to, over time, conserve taxpayer dollars. However, absent clear guidance and specifications for systems that use the PIV card, some manufacturers are absorbing substantial development costs to produce next generation systems that use the card. That work is being conducted without access to operational PIV credentials necessary to develop and test associated products.

Mr. Chairman, this situation is exacerbated by the fact that GSA has had to design a specification for the credential readers while developed product and service evaluation programs, a role it has never undertaken in the past.

The GSA approved product list is inferred from NIST documents which are substantially silent on the use of access control systems. Unfortunately, GSA restricts the approved products to being procured from GSA Schedule 70, an information technology schedule. This is unfortunate because physical access control systems and components are assigned to Schedule 84, where they have always been.

Multiple schedules make it difficult, both for the manufacturers developing and submitting products and the Government purchaser attempting to assemble the systems. HSPD–12 products need to be available from both Schedule 70 and Schedule 84.

Despite challenges, some agencies are doing an exemplary job of providing credentials for employees and upgrading their infrastructure to meet the requirements of HSPD–12.

In conclusion, SIA offers the following recommendations:

SIA encourages this subcommittee to direct OMB to establish, within its Office of E-Government Information Technology, a dedicated team of professionals who possess substantial knowledge of physical security technologies and applications. This team would support the ongoing efforts of the Interagency Security Committee [ISC], which is charged with developed physical security policies, standards, and strategies.

We also recommend that OMB establish a policy for implementation of physical security similar to its policy establishing guidance for the processes leading up to the issuance of the PIV II credentials. The policy must recognize that the PIV card is not compatible with most installed base packs currently in use, and the packs will have to be, at a minimum, upgraded, and most likely replaced.

Finally, we encourage you to consider SIA as a resource for the effective use of the PIV credential with physical access control systems.

Thank you for the opportunity to testify today.

[The prepared statement of Mr. Zivney follows:]

Statement by the Security Industry Association before the U.S. House Subcommittee on Government Management, Organization, and Procurement

April 9, 2008

Chairman Towns, Congressman Bilbray, and members of the subcommittee. Thank you for the opportunity to testify before you about federal agency implementation of Homeland Security Presidential Directive 12 (HSPD-12).

My name is Rob Zivney. I am the vice president of marketing for Hirsch Electronics headquartered in Santa Ana, California. Hirsch Electronics is a manufacturer of physical access control systems for non-residential markets, including the federal government. I also serve as the Chair of the Security Industry Association's (SIA's) Personal Identity Verification (PIV) Working Group.

I am honored to testify today on behalf of SIA, which represents 400 manufacturers, integrators, and dealers of electronic security equipment. SIA members provide electronic systems solutions for physical security that protect your constituents and millions of Americans who access government facilities, ports, local schools, colleges, hospitals, airports, mass transit systems, retail establishments, and other institutions. Many systems have the ability to change operational modes in response to varying threat levels to ensure the security of these facilities and the people within.

As this subcommittee examines the findings of the General Accountability Office (GAO) Report released earlier today, I would like to emphasize that SIA members strongly support the goals of HSPD-12. We welcome this subcommittee's interest in implementation of HSPD-12. SIA members are fully committed to offering our assistance to ensure the successful implementation of this directive by <u>all</u> federal agencies.

Mr. Chairman, I would like to make several points that will contribute to this subcommittee's evaluation of HSPD-12 implementation. Simply put, security is only as strong as the weakest link. In our view, HSPD-12 - and the associated standards developed by the National Institute of Standards and Technology (NIST), specifically the identity vetting processes - forms a far stronger foundation for our federal government agencies' security than we have ever witnessed in the past. Identity verification in routine access transactions are enhanced by the use of the credential bearer's fingerprints template, which are taken from the same fingerprints submitted for and cleared in the background check during the issuance process.

SIA believes the PIV II technical requirements for the implementation of HSPD-12 require an investment both financially and in the development of new infrastructure. However, the scope of the investment and time required for implementation were underestimated by the government when it set goals for the deployment of HSPD-12 through Office of Management and Budget (OMB) Memorandum M-05-24. Traditionally the functions of authentication and authorization have resided locally with

the administrator of the physical access control system (PACS). The HSPD-12 and Federal Information Processing Standard (FIPS) 201 model have changed this: the credential issuer to a large degree now handles authentication while authorization remains a function of the PACS. This has created a unique challenge facing federal agencies, the development of a substantial shared infrastructure to accommodate the increased functionality and security features of the PIV II credential. For many agencies, the development of this new infrastructure presents a significant learning curve that they are working diligently to overcome.

Mr. Chairman, the implementation of HSPD-12 is truly a pioneering effort on behalf of the federal government. It requires that the human resources, information technology, and security departments interface and cooperate on an unprecedented level. These three disciplines traditionally are different in cultures and basic objectives. This creates challenges for all parties involved in implementing HSPD-12.

Although HSPD-12 may not draw the attention of our nation's major media outlets, the world is watching. HSPD-12 is truly transformational. The issuance of OMB Memorandum M-05-24 was a bold move. In spite of the technical and procedural challenges, the subcommittee should note that there has been enough early success to attract scrutiny of HSPD-12 by other nations, state and local governments and other industry sectors.

Mr. Chairman, some may question the value of the PIV II credential because of the significant cost differential compared to traditional security technologies and the additional integration efforts required. How ever, the use of an identity credential coupled with the use of fingerprints for authentication of the bearer and the use of digital certificates and Public Key Infrastructure (PKI), promises to revolutionize government, significantly increase security, and conserve taxpayer dollars.

The methods and technologies needed to utilize the capabilities of the PIV II credential in a logical or physical access control system are still being discovered and developed. In the absence of clear guidance and specifications for the systems that will use the PIV card, some manufacturers have stepped up to the challenge and absorbed substantial research and development costs to produce next generation equipment capable of utilizing the features of a PIV II credential. These costs have been significant and made progress difficult as this work has been conducted without the benefit of having operational PIV II credentials available to manufacturers to develop and test associated products.

Mr. Chairman, given this subcommittee's oversight responsibility over the General Services Administration (GSA), you will be interested to know that this situation is exacerbated by the fact that the GSA has had to design a specification for the credential readers, and is testing to that specification, a role it has never undertaken in the past. As a result, the GSA Approved Product List (APL) testing program had to be created from scratch. The test specifications had to be inferred from the NIST specifications that were silent on the logical and physical access control systems that would actually use the

cards and card production apparatus. This made for a very lengthy process, which was challenging for both GSA and the manufacturers submitting equipment for evaluation. There is also a catch 22; only federal employees and contractors are authorized to possess PIV cards. However, manufacturers need PIV cards to develop products that will use the cards. Operational card stock for R&D and testing remains a key priority for the electronic security industry, due to the many options and variations allowed for in the NIST specifications.

GSA's current implementation of the approved products restricts these items to procurement from GSA Schedule 70, the Information Technology Schedule. However, the majority of the physical access control system components are assigned to Schedule 84, where they have always been. This makes it difficult both for the manufacturers submitting products and the government purchasers attempting to assemble systems from multiple GSA schedules. The decision to place the new PIV components "exclusively" on Schedule 70 was mandated by OMB. We believe this subcommittee should encourage the dual listing of approved HSPD-12 products on both Schedule 70 and Schedule 84 to serve both the IT security and physical security needs of agencies.

Despite challenges, SIA finds there are some agencies doing an exemplary job of provisioning credentials for their employees and upgrading their infrastructure to meet the requirements of HSPD-12. For those agencies that continue to work to improve their implementation of HSPD-12, SIA has formed a Government Infrastructure Security End User Group to assist in this process.

This SIA group serves as a bridge between industry and government and it is a conduit for information between these two entities. Over the past several months SIA has conducted non-product-specific training for federal employees to try to shorten the learning curve that agency security personnel are experiencing. These interactive sessions provide our industry with a means to learn about the needs of federal agencies. This helps our members develop products that meet those needs. I am pleased to say that this training is provided by SIA at no cost to federal employees. It is intended to help develop a federal security workforce that is better informed about physical security technologies so that the goal of maximizing tax dollars to provide security for government facilities is met.

Mr. Chairman, as part of SIA's efforts to advance HSPD-12 implementation, we have proactively engaged NIST in extensive conversations related to FIPS-201 and its supporting Special Publications. SIA's PIV Working Group also serves as a mechanism to quickly address government technical needs or questions related to physical security infrastructure. SIA also is an active participant in the Government Smart Card Interagency Advisory Board (IAB) and we take every opportunity to help government understand the ramifications of HSPD-12 on currently deployed security and life safety technologies as well as future technologies. We regularly and consistently provide comments on new and revised draft NIST publications that are posted for public review. In addition, we sponsor workshops and briefing sessions for industry, often with the

participation of GSA, NIST, and other agencies involved with the development and implementation of the standards.

In conclusion, SIA would like to offer additional recommendations for the subcommittee's consideration that may expedite full implementation of HSPD-12:

First, we would encourage this subcommittee to direct OMB to establish a dedicated team of professionals within its Office of E-Government and Information Technology. These employees have substantial knowledge of physical security technologies and physical security infrastructure within federal agencies.

This proposed OMB "physical security team" should regularly coordinate with the private sector toward implementation of HSPD-12 and the development of future Executive Branch policies and directives that may impact physical security at government facilities. As part of its responsibilities, this physical security team of experts would support the ongoing efforts of the Interagency Security Committee (ISC) that is charged with developing physical security policies, standards, and strategies at non-military government facilities. Established in 1995 under Executive Order 12977, the ISC is chaired by the Department of Homeland Security and comprised of senior level officials from federal government agencies.

Secondly, we recommend that OMB establish a policy for implementation of physical security similar to the policy document M-05-24. We have progressed to date with an "unfunded mandate" for PIV-I and PIV-II. However, physical access control systems are outside of that scope, and as such have neither funding nor a mandate. This requested policy must recognize that the PIV card is not compatible with most installed PACS currently in use and that the PACS will have to be, at a minimum, upgraded or, most likely, need to be replaced.

Finally, we encourage you to consider SIA as a resource for the effective utilization of the PIV credential with physical access control systems. We not only have the skills and knowledge for deployment and use, but are also an ANSI standards development organization (SDO). As such we are able to produce standards for physical security systems and indeed have many such applicable standards in development now.

Thank you for the opportunity to testify before you and the subcommittee. I applaud your interest in this important initiative and look forward to answering your questions.

Mr. TOWNS. Thank you very much.
Mr. Romero, 5 minutes.

STATEMENT OF BENJAMIN ROMERO

Mr. ROMERO. Good afternoon, Mr. Chairman, ranking member, my name is Ben Romero, and I speak to you as the chairman of the Intelligence Committee of the Information Technology Association of America and on behalf of the Security Clearance Reform Coalition.

Thank you for this opportunity to discuss a reform of the current granting process. In addition to these oral comments, I ask that the committee accept our attached written recommendations that expand upon the issues we feel are critical to addressing this persistent problem.

Industry has used a simple mantra to explain what we believe will bring about transformation of the clearance granting process. One application, one investigation, one adjudication, and one clearance. We seek an internet-based application that collects information electronically and forms the basis for an end-to-end digital process that creates a record that can be amended by investigators, adjudicators, and security officers for the life of the clearance, an investigation that would be timely, uniform, and thorough in its processed end product, an adjudication where an applicant is judged using updated, viable, post-cold-war criteria, and a clearance that is accepted across the Federal Government with minimal additional vetting.

In looking at the clearance granting process and its effectiveness, the committee should examine the reports of the industry-led working group of the National Industry Security Program Policy Advisory Committee, which recently analyzed actual results from clearance processed through DSS and DISCO. This task force found that, on average, secret clearances took more than 200 days, top secret clearances took more than 300 days to process in 2007. This was an end-to-end analysis measuring from the time an applicant was given access to complete the online SF–86 provided on the electronic questionnaire for investigative processing Web site, e-QIP, to the point when the adjudicators determine whether or not a clearance was granted.

Even more alarming is the finding of the working group regarding investigations for top secret clearances, where the trend line has grown to more than a year, and currently tops out at 540 days.

There are a number of conditions that bear mention because they are impacting the effectiveness of the end-to-end process. These include an inability to accurately forecast budget needs in some agencies, an inability in most applications to accept electronic attachments like release forms and digital fingerprints, an inability to identify additional case codes that frequently cause a case to be reopened for further investigations and the out-of-sync applications used in e-QIP.

Industry believes that many of the problems that cause delays with the current process are rooted in the investigative stage. These include the ineffective marriage of e-QIP applications with fingerprint cards and release forms, too much touch labor in the investigative stage of the process, including printing of electronic

records, because PIPS is incapable of saving attachments like criminal or electronic records—they bar code and scan documents rather than use two electronic records—and the mailing of investigative files back and forth between OPM and their field investigators.

The subcommittee has highlighted today an issue industry has long noted with concern. While we fully support HSPD–12 and the effort to create greater assurance for all Government employees and contractors through new identification measures, we have been concerned about the sapping of resources for the underlying investigations. HSPD–12 background checks are national agency checks with local agency checks, very similar to the level of commitment of resources for secret clearances. We have been concerned that this would be insufficient Government resources to adequately devote to the HSPD–12 checks, while working to improve the clearance process.

It is our hope that all those holding current positions of trust that require the NAC check or greater will be approved under that portion of HSPD–12.

We are cognizant of what is going on in OSD, OPM, ODNI as they try to revamp the clearance. We are behind it 100 percent.

The nine associations of the Security Clearance Reform Coalition again thank the subcommittee for the opportunity to highlight our perspectives in these deliberations, and we hope that 2008 will finally be the year that we see solutions implemented.

Thank you, sir.

[The prepared statement of Mr. Romero follows:]

Testimony of the

Security Clearance Reform Coalition

Submitted to the Subcommittee on Government Management, Organization and Procurement
of the House Oversight and Government Reform Committee
April 9, 2008

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council

SECURITY CLEARANCE REFORM COALITION
TESTIMONY BEFORE THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION AND PROCUREMENT OF THE HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
APRIL 9, 2008

The Security Clearance Reform Coalition[1] would like to thank the Subcommittee for this opportunity to convey our perspective on the issues and concerns surrounding reform of the clearance granting process.

Industry has used a simple mantra to explain what we believe will bring about transformation of the clearance granting process: one application, one investigation, one adjudication and one clearance. We seek an internet-based application that collects information electronically and forms the basis for an end-to-end digital process that creates a record that can be amended by investigators, adjudicators and security officers for the life of that clearance; an investigation that would be timely, uniform and thorough in its process and product; an adjudication where an applicant is judged using updated, viable post-Cold War criteria; and, a clearance that is accepted across the Federal government with minimal additional vetting.

In evaluating the clearance granting process and its effectiveness, the Committee should examine the reports of an industry-led working group of the National Industrial Security Program Policy Advisory Committee (NISPPAC), which recently analyzed actual results from clearances processed through Defense Security Service and the Defense Industrial Security Clearance Office (DISCO). This task force found that on average, Secret clearances still took more than 200 days and Top Secret clearances took more than 300 days to process in 2007. This was an end to end analysis measuring from the time an applicant was given access to complete the online SF-86 provided on the Electronic Questionnaires for Investigations Processing website (e-QIP) to the point when the adjudicators determined whether or not a clearance was granted. Even more alarming is the finding of the working group regarding reinvestigations for Top Secret clearances, where the trend line has grown for more than a year and currently tops out at 540 days. As you know, reinvestigations are the periodic reviews of the current clearance holders and these delays impact the ability of current employees to continue working on National Security programs. These findings are the most current and thorough evaluation of the process and gives empirical backing to the anecdotal experiences industry has been reporting for years.

There are a number of conditions that bear mention because they are impacting the effectiveness of the end to end process and undermining the ability of government and industry to maintain and build a sufficient number of skilled, cleared personnel for the National Security mission. These include: an inability to accurately forecast budget needs in some agencies; an inability in most applications to accept electronic attachments, like release forms and digital fingerprints; an inability to identify additional case codes that frequently cause a case to be re-opened for further investigation; and, "out-of-sync" applications using e-QIP.

While there have been some improvements in the budget forecast, problems will remain and the impact they have will persist as long as the process is reliant upon estimates and voluntary

[1] The Security Clearance Reform Coalition is comprised of the Aerospace Industries Association, the American Council of Engineering Companies, AFCEA International, the Associated General Contractors of America, the Association of Old Crows, the Information Technology Association of America, the Intelligence and National Security Alliance, the National Defense Industrial Association and the Professional Services Council.

disclosures of information. Some of the necessary information is resident or available elsewhere and could be captured to enhance the accuracy of the estimation.

Several of the issues raised are technical in nature, but have a very significant impact on the efficiency of the process and the ability to create a record that can be used for the life of the clearance. For example, it is imperative that government rapidly move to automate the collection of digital fingerprints and signatures and allow these digital records to be appended to the e-QIP electronic application. The Department of Homeland Security has accomplished this with the TWIC identification program for port workers, so we should be able to accomplish this same task in the IC and defense and civilian agencies. This failure of the process is a significant roadblock and correcting it will save weeks or months in the processing time for an application, as the process now is heavily reliant upon mailing paper documents and marrying those documents with a printout of the electronic application. Why would we continue a process that requires us to print a 30+ page application when we already have it in electronic format?

Industry believes that many of the problems that cause delays with the current process are rooted in the investigative stage. These include: the inefficient marriage of e-QIP applications with fingerprint cards and release forms; too much touch labor in the investigative stage of the process, including printing of electronic records because PIPS is incapable of saving attachments like criminal or electronic records; bar-coding and scanning (imaging) of documents rather than using a truly electronic record and the mailing of investigative files back and forth between OPM and field investigators.

The Subcommittee has highlighted today an issue we have long noted with concern in industry. While we fully support HSPD-12 and the effort to create greater assurances for all government employees and contractors through new identification measures, we have been concerned about the sapping of resources for the underlying investigations. HSPD-12 background checks are a National Agency Check with Local Agency Check (NACLC), very similar to the level of commitment of resources for a Secret clearance. We have been concerned that there will be insufficient government resources to adequately devote to HSPD-12 checks, while working to improve the clearance process.

While these issues are roadblocks in the current process and must be addressed to solve short-term needs, industry is fully supportive of the calls of the Congress for a transformation of the process. To that end, we commend the President for his February 5, 2008 memo that called for the submission of a plan to transform the clearance granting process no later than April 30, 2008. This memo memorializes the activity of a Joint Task Force coordinated by the Office of Management and Budget (OMB), the Undersecretary of Defense for Intelligence (USD(I)), the Director of OPM and the Office of the Director of National Intelligence (ODNI). This task force has proceeded under the premise that we need to bring transformation to the way we determine whether or not someone is trustworthy enough to handle the Nation's critical information. The effort would change what we ask, how we ask it and the way we grant and maintain clearances once granted. This approach is different because it does not seek to fix

the parts of the broken process we use today, but instead creates a new, more efficient process going forward.

Industry has been apprised of the work of this group and we fully support this initiative. The Tiger Team intends to use technology to create an end-to-end, automated, interoperable process that collects information in new and different ways and takes advantage of government and commercial databases to expedite the application, investigation and adjudication stages of the process. Using these technologies in these new ways will also facilitate reciprocity. While industry is optimistic about the work of this Tiger Team and waits to evaluate their report in April, further action is needed now.

Congress should be cognizant of the fact that some will oppose these changes and should take every effort to prevent the success of such efforts. For example, counter-intelligence concerns abound and, while not to be ignored, must be tempered with the desire to understand and mitigate risk, not seek to avoid it entirely. Others will fight to preserve the current process because it is the business case for their agency or office and is the reason for their existence. But change is inevitable and, in the case of clearance reform, must be allowed to happen.

The IRTPA was passed by the Congress in 2004 – and the delays in the clearance granting process have been recognized for decades – so the President's call for a plan should be the last. Further delays – be they bureaucratic, legislative or budgetary – should no longer be tolerated. We must move beyond additional calls for plans and begin to actually make investments to change the process. Congress should support the efforts of the Tiger Team, take action to see that they are not delayed by bureaucratic roadblocks and that they have the resources to initiate their vision for transforming the process.

The nine associations of the Security Clearance Reform Coalition again thank the Subcommittee for this opportunity to highlight our perspectives in this deliberation. We hope that 2008 will finally be the year that we see solutions implemented.

Recommendations of the

Security Clearance Reform Coalition For Improvements to the Clearance Granting Process

Presented to the Government Management, Organization and Procurement Subcommittee
Of the House Oversight and Government Reform Committee
April 9, 2008

Aerospace Industries Association
American Council of Engineering Companies
Armed Forces Communications & Electronics Association
Associated General Contractors of America
Association of Old Crows
Information Technology Association of America
Intelligence and National Security Alliance
National Defense Industrial Association
Professional Services Council

While many of these recommendations are focused on the collateral clearance granting process and many of the IC agencies are running efficient processes using state of the art technologies, making these improvements would significantly improve the process for all government and industry users.

These recommendations are based upon extensive interviews with the various stakeholders in the clearance granting process to better understand what happens to an application as it moves through the process and are bolstered by the numbers of clearances in the backlog, defined as non-compliant with the metrics of the 2004 Intelligence Reform and Terrorism Prevention Act.

APPLICATIONS

1) End-to-End Capability: The process is one large paper shuffle and must adopt an end-to-end capability to share data interoperably in real-time. No such planning is currently underway, as there is no one manager for the process.

2) Require Electronic Applications: OPM must enforce the requirement published in the Federal Register requiring all new applications and renewals to be submitted via the Internet-based e-QIP. Currently, between 25-40% of all applications are still accepted in hard copy. Several major agencies, including the General Services Administration, still require applicants to complete paper applications and include other extraneous information, like resumes, as part of the application.

3) Clarify Metrics: Congress must clarify that the time frames established in the IRTPA for clearance processing begin when an application is actually received by the investigative agency, regardless of when it is actually scheduled. Frequently, the calendar for the investigation is not started until months after the application has been received by the investigative agency. Congress should also clarify the metrics to remove the ability to "mask" true status of the effectiveness of the process by requiring reporting based upon all cases in the pipeline, instead of an artificial 80% of the best cases.

4) Improve JPAS: DoD must invest the funds necessary to make required improvements to JPAS. This is not happening at present and service is being degraded to the DoD adjudication facilities as well as to thousands of security managers in both government and industry who depend upon it for mission requirements. The JPAS user community and the Defense Security Service (DSS) have already identified the changes needed to streamline and accelerate JPAS processing, but the level of priority for this problem seems to have fallen since last summer when DSS ran out of funding. These improvements include the ability to accept and capture digitized fingerprints and signatures from industry and eliminate delays and dropped applications caused by JPAS being out of synch.

INVESTIGATIONS

1) Modernize Data Capture: OPM must modernize its data capture procedures. Imaging, while frequently cited as an "automation" of the clearance process, is nothing more than taking a picture of a document and is ineffective at capturing the data in the document for use in an information technology system.
   a. OPM must stop accepting fingerprint cards and start using digitized fingerprint capture tools such as LiveScan.
   b. Signatures on release forms can also be easily captured using technology at checkout counters across America and eliminates the need to print and mail release forms to investigators when needed.
   c. Investigative files are also selectively imaged, where using truly digitized information would allow for the preservation of the entire file, not just summaries, and preserve critical information like credit reports and criminal histories.

2) Modernize Data Management at OPM: OPM-FISD continues to rely upon PIPS, an antiquated stand-alone mainframe computer system that is not interoperable and cannot be made so. This reliance forces continuation of labor-intensive paper handling that significantly delays the processing of clearances. Many of the problems identified by industry in the process are related to or stem from this reliance upon PIPS.
   a. PIPS does case assignment, but once a case is assigned, it is printed out and mailed to investigators for processing.
   b. For paperwork management, OPM relies upon barcodes, which are manually keyed, printed and affixed to documents in the hard copy files.
   c. Only some of the information collected during an investigation is preserved for future review or access by the adjudicators. Critical information sources, such as criminal and credit histories, are not retained.
   d. CVS is an important tool, but cannot adequately verify a clearance since it relies upon batched data and is not real-time.

3) Eliminate the "Closed Pending" status for clearances at OPM: OPM categorizes investigations that are incomplete due to the lack of some data or incomplete status of some component of the application as "closed pending." Some of these incomplete files are then passed to the originating agency for adjudication, while other departments, like DoD, refuse to accept or adjudicate these applications in "closed pending" status. Since this information is frequently needed to make adjudicative risk assessments, agencies are then forced to return the application to OPM, thereby incurring further charges to process the clearance.

4) Implement the Use of Phased Periodic Reinvestigations (PR): The federal government should direct implementation of phased periodic reinvestigation (currently being implemented only by DoD) to realize the full benefits of scaling the PR in such a way that limits the use of costly and time consuming field investigation. Using commercial and government databases, cleared personnel are evaluated for any activity that would

require further investigation (Phase I). If the Phase I results (automated checks and selected interviews) are favorable, there is no need to proceed to the costly field investigation (Phase II). Phased PR's can be conducted more frequently with less cost, so that the cleared personnel – those most in a position to cause harm to the United States – are more effectively monitored. It is conservatively estimated that such an approach could save 20% or more of the cost of conducting periodic reinvestigations.

ADJUDICATIONS

1) Adequately Develop Derogatory Information: OPM has modified the criteria to which clearances at various levels are investigated, including dropping efforts to investigate and develop derogatory information for Secret collateral clearances. Such a change in the process makes it difficult if not impossible to effectively adjudicate many applications.

2) Enhance Training Standards: Develop and implement standardized professional training and certification criteria for adjudicators across the federal government. This would create equity in the training and development of adjudication officers and improve reciprocity of clearances by building trustworthiness across federal agencies with the application of adjudicative standards.

3) Establish Common Recordkeeping: Establish and implement a common approach across all agencies, using existing central clearance databases like CVS, JPAS, and Scattered Castles, for the recording of waivers, conditions, and deviations in order for adjudicators and security officers to have access to this information when taking an action to reciprocally accept another agency's clearance or access determination.

RECIPROCITY

1) Increase Clearance Data Sharing: Intelligence Community agencies should be required to populate JPAS with clearance/access information on non-classified employees. All such data should be validated to ensure that it is not corrupting critical, accurate information about existing clearance holders contained in the databases.

2) Reinforce Uniformity in the Application of Reciprocity: Some Intelligence Community agencies are requiring that a clearance must be "active" rather than "current" before it will be considered for acceptance under reciprocity rules. This approach necessitates obtaining the prior investigative file and re-adjudicating the clearance. This is a costly, time consuming and unnecessary process under existing policy and is in violation of the spirit, if not the letter, of the IRTPA. It is also in direct conflict with the provisions of EO 12968 and OMB memoranda of December 2005 and July 2006 (Checklist of Permitted Exceptions to Reciprocity) which require a valid "access eligibility determination."

3) Provide Access to JPAS for Authorized Agencies: All authorized Federal agencies should be given direct access to JPAS, as the sole system of record of the U.S. Government for all clearance and access eligibility determinations, in order to more fully and efficiently realize the goal of clearance/access reciprocity.

BUDGET AND PERSONNEL

1) Establish Efficient Budgetary Mechanisms: Budget issues were partly to blame for the processing moratorium on industry security clearances. As such, security clearance reform must include budget improvements as well. For instance, the federal government must develop a more accurate system for estimating the demand of industry clearances, and the appropriate agencies should submit budget requests that mirror the anticipated demand, with a limited reliance on charged premiums.

2) Enhance OPM Workforce Capabilities: Likewise, OPM's workforce capabilities must also be aligned to meet the anticipated demand for security clearances, as well as the demand for investigations of government and contractor personnel under HSPD-12 (industry estimates this requirement to include over 10M individuals). While some flexibility currently exists, industry is skeptical that it can meet these anticipated demands.

3) Build More Accountability Into the Invoicing Process for Clearances: OPM should not collect fees from the agency until the background check is completed and should provide greater clarity in their billing practices per the DoD IG investigation of these practices.

Mr. TOWNS. Thank you very, very much for your testimony.

Let me begin with you, Mr. Zivney. You propose that OMB establish a dedicated staff of security professionals to coordinate with the private sector on HSPD–12. The report from GAO leads me to think that OMB does need some help. Can you describe what advice you would give OMB right now in order to get the most out of HSPD–12 moving forward?

Mr. ZIVNEY. I think the focus has perhaps been on the hard part, and that was to get the cards out, get the infrastructure in place to issue the cards, and now we are really moving into phase two, and that is using the cards. If we are going to use the cards in a physical access control system, this takes skills that go beyond what you might often find in e-authentication or in focus group. And I know they are focused on issuing the card.

The disciplines of physical access control systems are different. I know there was some talk of authentication factors. We typically think of a card or a pin you type in on a keypad or a biometric as an authentication factor, and we see PKIs an enhancement to that, but we need to make sure that, from a physical security point of view, we normally have a threat level adjustment. We just want to add more factors and have that scaling.

Currently, FIPS 201 is silent on all the physical access control systems. We think that someone needs to provide a little better insight in there, and we need some focus. SIA would be glad to assist with some of that guidance, but if we are going to apply it and use it in physical access control systems, we need to have skill sets and disciplines and knowledge of those techniques.

Mr. TOWNS. All right. Thank you.

What do we do? What can we do to speed this up? I mean, I think that is what I am asking.

Mr. ZIVNEY. We are disappointed it has taken so long. I don't believe that there is a lack of urgency with anybody. I think it was a very bold move. As we said earlier, I believe, that NIST rushed out those specifications in 6 months. Perhaps we went too fast at times.

If we can involve more industry some time before specs are released, if we have comment periods that really seek to understand the comments of industry when they submit them, and more dialog at this point, we build on what we have laid on a foundation. I think we can move faster by slowing down a little bit at this point. I think someone made that statement. This is a good time to do an assessment and really focus on usage next while we are continuing to issue the cards.

Mr. TOWNS. Thank you very much.

Mr. Romero, it is clear that you consider security clearance reform to be an urgent issue and that it requires immediate attention. You described some changes that you say could be made quickly, changes that have already been made in some agencies, as you indicated. What are some of those possible changes? What are you talking about?

Mr. ROMERO. Well, sir, I believe that the biggest thing we can do, the best thing we could do, is scrap the process that we have right now and come out with one that really, truly uses IT. We are trying to use something that has been in existence for so many

years that what we are doing is taking baling wire and trying to keep it together so that it continues to process. When you go out and take fingerprint cards, scan them, then send them across ether and say that you are doing IT in today's world, we are not. We are still operating in yesterday's IT environment, or whatever the environment was.

I picked up my clear card here recently. My fingerprints were taken, my eye was taken. That can be used as things go forward. As we are looking at the checks, as we are improving the security clearances, there is all kinds of information that is out there available that is used by just about everybody else except the Government to find out if you are even qualified to hold a security clearance. They check all of us.

All our information is out there available to be checked, whether they are insurance records, whether they are Government records, whether they are tax records. All of those are accessible, but we don't touch those. We go out and ask questions that were asked and based on cold war era, asking my neighbor if I am a trustworthy American. I might not have talked to my neighbor but once in the past year because of the types of hours a lot of people hold.

That is the gist of what I am talking about, sir, where we are still operating in the past.

Mr. TOWNS. So basically you are saying that one size should fit all. Is that what you are saying?

Mr. ROMERO. Not necessarily. One size can fit all to start, and then you can add to it. If you have a basis, if you take the NAC as a basis and find out, hey, does that person have a drinking problem, hey, has his bank account really rapidly grown, those types of things that can be done very simply and easily to start with might grant you at least the initial level of clearance. Then, as you need more because you are going to be working—and I worked as an intelligence officer for most of my life—then they start asking additional questions and finding out more about your background to go from there.

Mr. BILBRAY. Mr. Chairman, can I be recognized?

Mr. TOWNS. I think it is your time now.

Mr. BILBRAY. I think the point is that maybe one size doesn't fit all, but the shoes all should be built in the same basic form, and then if they need to be used for duck hunting you modify them a little bit for this, or for deer hunting here, or for tennis you do this. So, in other words, there needs to be sort of a general production line that is upgraded that we are not going back and using some antiquated concepts. That is a real concern I have.

I saw how far California went in the 1970's by going to the Cal ID and getting digital readings of everybody that got a driver's license, which made huge breakthroughs, and so I am a big supporter of this. But the problem is getting them to get out of the paper and into electronic.

I have no real questions except for a comment. If there is anything that you guys see that we are not doing working with the private sector on this issue, we need to know about it, because we have seen what everybody else is doing.

I was appalled, Mr. Chairman, when we had the breach of the disc on our nuclear defense strategy disappear, and I was abso-

lutely blown out that you could actually go in to Livermore, pull it off the shelf, and there was no record of who was in the vault and there was not even an electronic reader telling you when the disc was taken out of the vault. When that disc leaves that shelf, that slot, it should say it is gone as of this time, and we should have a record of who is in the vault because they used electronic access that showed them in there. That would have been the most simple thing in the world to take care of if we had the right data bases and the right type of inventory control using electronics rather than depending on antiquated World War II technology.

Thank you very much. I actually think that this issue goes a lot farther. I have been discussing with the White House why all Federal identification in the United States is not upgraded to the real ID standard that we set for the others, including the Social Security card.

If there was going to be an embarrassment, Mr. Chairman, explaining to your children or your grandchildren why we are still using a piece of paper and a number as our No. 1 ID for employment in this country, that has not been upgraded since 1937. I sure tell you I start understanding why people think there is a conspiracy in this country not to protect us because how do you justify that. I can't think of a State or a private sector that would justify having a piece of paper and a number as its foundation of identification.

Any comments before we relieve you gentlemen? Does the chairman have some more questions?

Mr. TOWNS. No. I am actually finished, just to say to you, though, that when you say Social Security, you would be amazed at how many people are walking around that do not have one and have not had one in many, many years. I think you would be amazed.

Mr. BILBRAY. I am not. I haven't had once since I was a lifeguard.

Mr. TOWNS. How many people in the room have a Social Security card in your pocket? Raise your hand.

[Show of hands.]

Mr. BILBRAY. By the way, they recommend you never, never carry your Social Security card around. Never. That is the No. 1 no-no, because you have your credit cards, your ID, and your social. Forget it.

Mr. TOWNS. Just remember your number.

Let me thank you. I really appreciate your coming in. Your entire statement will be placed in the record. Of course, if you have any other suggestions or comments, we would definitely appreciate it.

I agree with you. I think that there is a desire to move forward. I don't question the witnesses that were before us today in terms of their commitment and their dedication. But something is wrong that we can't move forward. I am not sure what it is. That is the whole thing.

I think you helped us some, because when you look at the fact that we only have 3 percent, and I think the commitment and dedication is there, but something else is missing. Maybe you guys can help us figure out what that is and be able to move it forward.

I want to thank you again for coming. We appreciate your testimony.

The hearing is adjourned.

[Whereupon, at 3:45 p.m., the subcommittee was adjourned.]

○