

September 2011

PERSONAL ID VERIFICATION

Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards

U.S. Government Accountability Office

GAO 90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

Why GAO Did This Study

To increase the security of federal facilities and information systems, the President issued Homeland Security Presidential Directive 12 (HSPD-12) in 2004. This directive ordered the establishment of a governmentwide standard for secure and reliable forms of ID for employees and contractors who access government-controlled facilities and information systems. The National Institute of Standards and Technology (NIST) defined requirements for such personal identity verification (PIV) credentials based on “smart cards”—plastic cards with integrated circuit chips to store and process data. The Office of Management and Budget (OMB) directed federal agencies to issue and use PIV credentials to control access to federal facilities and systems. GAO was asked to determine the progress that selected agencies have made in implementing the requirements of HSPD-12 and identify obstacles agencies face in implementing those requirements. To perform the work, GAO reviewed plans and other documentation and interviewed officials at the General Services Administration, OMB, and eight other agencies.

What GAO Recommends

GAO is making recommendations to nine agencies, including OMB, to achieve greater implementation of PIV card capabilities. Seven of the nine agencies agreed with GAO’s recommendations or discussed actions they were taking to address them; two agencies did not comment.

PERSONAL ID VERIFICATION

Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards

What GAO Found

Overall, OMB and federal agencies have made progress but have not fully implemented HSPD-12 requirements aimed at establishing a common identification standard for federal employees and contractors. OMB, the federal Chief Information Officers Council, and NIST have all taken steps to promote full implementation of HSPD-12. For example, in February 2011, OMB issued guidance emphasizing the importance of agencies using the electronic capabilities of PIV cards they issue to their employees, contractor personnel, and others who require access to federal facilities and information systems. The agencies in GAO’s review—the Departments of Agriculture, Commerce, Homeland Security, Housing and Urban Development, the Interior, and Labor; the National Aeronautics and Space Administration; and the Nuclear Regulatory Commission—have made mixed progress in implementing HSPD-12 requirements. Specifically, they have made substantial progress in conducting background investigations on employees and others and in issuing PIV cards, fair progress in using the electronic capabilities of the cards for access to federal facilities, and limited progress in using the electronic capabilities of the cards for access to federal information systems. In addition, agencies have made minimal progress in accepting and electronically authenticating cards from other agencies.

The mixed progress can be attributed to a number of obstacles agencies have faced in fully implementing HSPD-12 requirements. Specifically, several agencies reported logistical problems in issuing credentials to employees in remote locations, which can require costly and time-consuming travel. In addition, agencies have not always established effective mechanisms for tracking the issuance of credentials to federal contractor personnel—or for revoking those credentials and the access they provide when a contract ends. The mixed progress in using the electronic capabilities of PIV credentials for physical access to major facilities is a result, in part, of agencies not making it a priority to implement PIV-enabled physical access control systems at all of their major facilities. Similarly, a lack of prioritization has kept agencies from being able to require the use of PIV credentials to obtain access to federal computer systems (known as logical access), as has the lack of procedures for accommodating personnel who lack PIV credentials. According to agency officials, a lack of funding has also slowed the use of PIV credentials for both physical and logical access. Finally, the minimal progress in achieving interoperability among agencies is due in part to insufficient assurance that agencies can trust the credentials issued by other agencies. Without greater agency management commitment to achieving the objectives of HSPD-12, agencies are likely to continue to make mixed progress in using the full capabilities of the credentials.

Contents

Letter		1
	Background	3
	OMB and Agencies Have Made Progress but Have Not Yet Fully Implemented Homeland Security Presidential Directive 12	15
	Agencies Face Obstacles in Fully Implementing Homeland Security Presidential Directive 12	32
	Conclusions	40
	Recommendations for Executive Action	41
	Agency Comments and Our Evaluation	41
Appendix I	Objectives, Scope, and Methodology	45
Appendix II	Requirements and Components of PIV-II	47
Appendix III	Selected NIST Guidance	49
Appendix IV	Recommendations to Departments and Agencies	53
Appendix V	Comments from the Department of Commerce	57
Appendix VI	Comments from the Department of Homeland Security	58
Appendix VII	Comments from the Department of Housing and Urban Development	60
Appendix VIII	Comments from the Department of the Interior	62

Appendix IX	Comments from the Department of Labor	64
Appendix X	Comments from the National Aeronautics and Space Administration	66
Appendix XI	Comments from the Nuclear Regulatory Commission	68
Appendix XII	GAO Contact and Staff Acknowledgments	69
Table	Table 1: Examples of Approved PIV Card Authentication Capabilities and Their Associated Assurance Levels	10
Figures	Figure 1: A PIV Card Showing Major Physical Features	8
	Figure 2: Agencies' Progress in Completing Background Checks from 2008 and 2011	20
	Figure 3: Agencies' Progress in Completing Background Checks by Personnel Groups as of March 2011	21
	Figure 4: Agencies' Progress in Issuing PIV Cards from 2008 and 2011	24
	Figure 5: Agencies' Progress in Issuing PIV Cards by Personnel Groups as of March 2011	25

Abbreviations

CHUID	cardholder unique identifier
CIO	chief information officer
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
HUD	Department of Housing and Urban Development
ID	identification
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
PACS	physical access control system
PIN	personal ID number
PIV	personal identity verification
PKI	public key infrastructure
SP	special publication
USPTO	U.S. Patent and Trademark Office
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. The published product 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.



G A O

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 20, 2011

Congressional Requesters

In an effort to increase the security of federal facilities and information systems where there is potential for terrorist attacks, the President issued Homeland Security Presidential Directive 12 (HSPD-12) in August 2004. This directive ordered the establishment of a mandatory, governmentwide standard for secure and reliable forms of identification (ID) for federal government employees and contractor personnel who access government-controlled facilities and information systems.

In February 2005, the Department of Commerce's National Institute of Standards and Technology (NIST) issued the original version of Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*.¹ Known as FIPS 201, the standard sets out requirements for background checks, as well as issuing and using credentials based on interoperable smart cards.² The Office of Management and Budget (OMB) directed that by October 27, 2007, agencies issue and require the use of FIPS 201-compliant credentials, called personal identity verification (PIV) cards, by all employees and contractor personnel who had been with the agencies for 15 or fewer years. It also directed that the remainder of the employees be issued cards and begin using their cards no later than October 27, 2008.³

¹In March 2006, NIST issued a revised version of its standard, FIPS 201-1.

²Smart 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 but cannot process information. Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

³OMB, *Memorandum for the Heads of All Departments and Agencies: Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, M-05-24 (Washington, D.C.: Aug. 5, 2005); and *Memorandum for the Heads of All Departments and Agencies: HSPD-12 Implementation Status*; M-08-01 (Washington, D.C.: Oct. 23, 2007).

We previously reported on agencies' progress toward implementing HSPD-12 requirements.⁴ This report responds to your request that we (1) determine what progress agencies have made in implementing HSPD-12 requirements, and (2) identify obstacles agencies faced in implementing those requirements.

To address these objectives, we conducted audit work at the same eight agencies we reviewed for our last report: the Departments of Agriculture (USDA), Commerce, Homeland Security (DHS), Housing and Urban Development (HUD), the Interior, and Labor; the National Aeronautics and Space Administration (NASA); and the Nuclear Regulatory Commission (NRC). These agencies have a range of experience in implementing smart-card-based ID systems. To obtain information on the agencies' progress, we analyzed documentation such as agencies' high-level plans for HSPD-12 implementation and documentation of their implementation activities, such as agencies' quarterly HSPD-12 status reports. To assess the reliability of the data collected from the eight agencies, we submitted questions to the agencies and reviewed agency documentation. In some cases, the data included were based on best estimates. We noted in the report when this was the case. We determined the data were sufficiently reliable for providing an overview of agency progress. We also interviewed program officials from these agencies, as well as General Services Administration (GSA) and OMB officials who have been involved in supporting implementation of HSPD-12 across the government.

We performed our work at Commerce, DHS, GSA, HUD, Interior, Labor, NASA, NRC, OMB, and USDA in the Washington, D.C., area from October 2010 to September 2011. We conducted this performance audit 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. Additional details of our objectives, scope, and methodology are provided in appendix I.

⁴GAO, *Electronic Government: Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards*, [GAO-08-292](#) (Washington, D.C.: Feb. 29, 2008); and *Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, [GAO-06-178](#) (Washington, D.C.: Feb. 1, 2006).

Background

Traditionally, the federal government has used a variety of access control techniques to protect its facilities and computer systems. Visual authentication of ID cards has typically been used as a way to control access to physical facilities. However, smart card technology can help authenticate the identity of an individual in a substantially more rigorous way than is possible with traditional ID cards. Such cards can provide higher levels of assurance for controlling access to facilities as well as computer systems and networks.

Access Control Techniques Provide Varying Levels of Assurance

Access control is the process of determining the permissible activities of users and authorizing or prohibiting activities by each user. Controlling a user's access to facilities and computer systems includes setting rights and permissions that grant access only to authorized users.

There are two types of access control: physical access and logical access. Physical access control focuses on restricting the entry and exit of users into or out of a physical area, such as a building or a room in a building. Physical access control techniques include devices such as locks that require a key to open doors or ID cards that establish an individual's authorization to enter a building. Logical access control is used to determine what electronic information and systems users and other systems may access and what may be done to the information that is accessed. Methods for controlling logical access include requiring a user to enter a password to access information stored on a computer.

Access control techniques vary in the extent to which they can provide assurance that only authorized individuals and systems have been granted access. Some techniques can be easily subverted, while others are more difficult to circumvent. Generally, techniques that provide higher levels of assurance are more expensive, more difficult to implement, and may cause greater inconvenience to users than techniques that provide lower levels of assurance. When deciding which access control mechanisms to implement, agencies must first understand the level of risk associated with the facility or information that is to be protected. The higher the risk level, the greater the need for agencies to implement a high-assurance-level access control system.

Smart Cards Can Provide Higher Levels of Assurance

One means to implement a high-assurance-level access control system is through the use of smart cards. Smart cards are plastic devices that are about the size of a credit card and contain an embedded integrated circuit chip capable of storing and processing data.⁵ The unique advantage that smart cards have over traditional cards with simpler technologies, such as magnetic strips or bar codes, is that they can exchange data with other systems and process information, rather than simply serving as static data repositories. By securely exchanging information, a smart card can help authenticate the identity of the individual possessing the card in a far more rigorous way than is possible with traditional ID cards. A smart card's processing power also allows it to exchange and update many other kinds of information with a variety of external systems, which can facilitate applications such as financial transactions or other services that involve electronic record-keeping.

In addition to providing ways to enhance security for federal facilities, smart cards also can be used to significantly enhance the security of an agency's computer systems by tightening controls over user access. Users wishing to log on to a computer system or network with controlled access must "prove" their identity to the system—a process called authentication. Many systems authenticate users by requiring them to enter secret passwords. This requirement provides only modest security because passwords can be easily compromised. Substantially better user authentication can be achieved by supplementing passwords with smart cards. To gain access under this scenario, a user is prompted to insert a smart card into a reader attached to the computer, as well as type in a password. This authentication process is significantly harder to circumvent because an intruder not only would need to guess a user's password but would also need to possess a smart card programmed with the user's information.

Even stronger authentication can be achieved by using smart cards in conjunction with biometrics. Smart cards can be configured to store biometric information (such as fingerprints or iris scans) in an electronic record that can be retrieved and compared with an individual's live biometric scan as a means of verifying that person's identity in a way that

⁵The term "smart card" may also be used to refer to cards with a computer chip that store information but do not provide any processing capability. Such cards, known as "stored value cards," are typically used for services such as prepaid telephone service or satellite television reception.

is difficult to circumvent. An information system requiring users to present a smart card, enter a password, and verify a biometric scan uses what is known as “three-factor authentication,” which requires users to authenticate themselves by means of “something they possess” (the smart card), “something they know” (the password), and “something they are” (the biometric). Systems employing three-factor authentication provide a relatively high level of security. The combination of a smart card used with biometrics can provide equally strong authentication for controlling access to physical facilities.⁶

Public Key Infrastructure Technology Can Further Enhance Access Control Based on Smart Cards

Smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions. PKI is a system of computers, software, and data that relies on certain cryptographic techniques to protect sensitive communications and transactions.⁷ A properly implemented and maintained PKI can offer several important security services, including assurances that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction.

PKI systems are based on cryptography and require each user to have two different digital “keys” to gain access: a public key and a private key. The public key is used to encrypt information, making it unintelligible to any unauthorized recipients. It is called “public” because it is made freely available to any users or systems that wish to be able to authenticate the user. To decrypt the information requires the private key, which is kept confidential on the user’s smart card. If a user’s card is able to successfully decrypt a message that was encrypted using the user’s public key, then the authenticity of the user’s smart card is proven. Public and private keys for PIV cards are generated by the card at the time it is issued.

⁶For more information about biometrics, see GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 15, 2002).

⁷For more information about PKI, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, [GAO-01-277](#) (Washington, D.C.: Feb. 26, 2001).

Security experts generally agree that PKI technology is most effective when used in tandem with hardware tokens, such as smart cards. PKI systems use cryptographic techniques to generate and issue electronic “certificates,” which contain information about the identity of the users, as well as the users’ public keys. The certificates are then used to verify digital signatures and facilitate data encryption. The certification authority that issues the certificates is also responsible for maintaining a certificate revocation list, which provides status information on whether the certificate is still valid or has been revoked or suspended. The PKI software in the user’s computer can verify that a certificate is valid by first verifying that the certificate has not expired, and then by checking the certificate revocation list or online status information to ensure it has not been revoked or suspended.

HSPD-12 Requires Standardized Agency ID and Credentialing Systems

In August 2004, the President issued HSPD-12, which directed Commerce to develop a new standard for secure and reliable forms of ID for federal employees and contractor personnel by February 27, 2005. The directive defined secure and reliable ID as meeting four control objectives. Specifically, the identification credentials were to be

- based on sound criteria for verifying an individual employee’s or contractor personnel’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 stipulated 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.

FIPS 201: Personal Identity Verification of Federal Employees and Contractors

In response to HSPD-12, Commerce’s 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 contractor personnel 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. The first part, called 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. The second part of the FIPS 201 standard, PIV-II, provides technical specifications for the implementation and use of interoperable smart cards in PIV systems.

Personal Identity Verification I

To verify individuals' identities, under PIV-I, agencies are directed to adopt an accredited⁸ identity proofing and registration process that is approved by the head of the agency. There are many steps to the verification process, such as completing a background investigation of the applicant, conducting 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.

Agencies are also directed to adopt an accredited card issuance and maintenance process that is approved by the head of the agency. This 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 the implementation and use of interoperable smart cards in PIV systems. The components and processes in a PIV system, as well as the identity authentication information included on PIV cards,

⁸NIST, *Guidelines for the Certification and Accreditation of PIV Card Issuers*, Special Publication 800-79-1 (Gaithersburg, Md.: June 2008), describes a set of attributes that should be exhibited by a PIV card issuer in order to be accredited.

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. Appendix II provides more information on the specific requirements and components of PIV-II.

Figure 1: A PIV Card Showing Major Physical Features



Source: GAO analysis of FIPS 201 guidance (data); Art Explosion, all rights reserved (seal).

The PIV cards contain a range of features—including a common appearance, security features, photographs, cardholder unique identifiers (CHUID), fingerprints, and PKI certificates—to enable enhanced identity authentication at different assurance levels. To use the enhanced electronic 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 the CHUIDs. Once acquired, these various devices need to be integrated with existing agency systems. For example, PIV system components may need to interface with human resources systems, so that when an employee resigns or is terminated and the cardholder's employment status is changed in the human resources systems, the change is also reflected in the PIV 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.

HSPD-12 guidance—including OMB guidance, FIPS 201, and other NIST guidance—allows for several different types of authentication that provide varying levels of security assurance. For example, simple visual authentication of PIV cards offers a rudimentary level of security, whereas verification of the biometric identifiers contained in the credential provides a much higher level of assurance. OMB and NIST guidance direct agencies to use risk-based methods to decide which type of authentication is appropriate in any given circumstance. Because visual authentication provides very limited assurance, OMB has directed that use of visual authentication be minimized. OMB guidance issued in February 2011 further stated that agencies were in a position to aggressively step up their efforts to use the electronic capabilities of PIV cards and should develop policies to require their use as the common means of authentication for access to agency facilities, networks, and information systems. Examples of approved methods for using PIV cards for authentication and associated assurance levels are described in table 1.

Table 1: Examples of Approved PIV Card Authentication Capabilities and Their Associated Assurance Levels

	Visual authentication only	CHUID authentication with visual authentication	Biometric authentication only	PKI authentication, and/or biometric authentication with visual authentication
Authentication capability	Visual authentication requires guards to examine the topographical features on the front and back of the PIV card. The guard checks to see that the PIV card appears to belong to the cardholder by comparing the photograph on the card with the cardholder. The guard is also required, among other things, to check the card's printed expiration date and verify the presence of security features that are meant to discourage tampering and falsification.	The CHUID is a number stored electronically on the card comprising several pieces of data, including the federal agency smart credential number, global unique identifier, expiration date, and digital signature. These components are used to authenticate the card and ensure that the card has not expired. Visual authentication of the card's security features and the photograph stored on the card are used to determine whether the card is genuine and whether it belongs to the individual using it.	PIV cards are directed to store two electronic fingerprints on the cards to allow live scans of the cardholders' fingerprints to be compared with previously stored fingerprint data to determine if there is a match.	The PIV card carries mandatory and optional asymmetric private keys and corresponding digital certificates that can be used for authentication. Using cryptographic functions, the certificates are verified, and the revocation status of the certificate is checked to ensure that the certificate has not been revoked.
Assurance level	Visual authentication alone does not provide an adequate level of assurance. Its effectiveness depends on the training, skill, and diligence of the guard. Counterfeit IDs can pass visual authentication easily, even when guards are well-trained. According to NIST, exclusive use of visual authentication may be appropriate only in limited circumstances, such as at a federal office that has very few employees.	Use of the CHUID combined with visual authentication provides more security assurance than visual authentication alone, because electronic means are used to authenticate the card. However, the CHUID is not encrypted, and thus there is some risk that a card may be forged.	Biometric authentication offers a high level of assurance of the cardholders' identity, even when there is no guard or attendant at the access point to perform visual authentication.	PKI can be used independently or in conjunction with both biometric and visual authentication. These methods offer a very high level of assurance in the identity of the cardholder. When used in combination, they offer the highest level of assurance available through a PIV card-based system.

Source: GAO analysis of FIPS 201 and related guidance.

In addition to the authentication capabilities discussed in table 1, 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.

Steps Taken by NIST,
OMB, and GSA to
Facilitate Agency
Acquisition of PIV Card
Systems and Issuance of
PIV Cards to Personnel

NIST issued several special publications that provide supplemental guidance on various aspects of the FIPS 201 standard, including guidance on verifying that agencies or other organizations have the proper systems and administrative controls in place to issue PIV cards and have the technical specifications for implementing the directed encryption technology. Additional information on NIST's special publications is provided in appendix III.

In addition, NIST 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 conformance with FIPS 201. These laboratories use the NIST test to determine whether individual commercial products conform to FIPS 201 specifications.

Once commercial products pass conformance testing, they must then go through performance and interoperability testing. GSA developed these tests to ensure that products and services meet FIPS 201 requirements. GSA tests products that have successfully passed NIST's conformance tests as well as other products as directed by FIPS 201 but which are not within the scope of NIST's conformance tests, such as PIV card readers, fingerprint capturing devices, and software directed to program the cards with employees' data. Products that successfully pass GSA's conformance tests are included on its list of products that are approved for agencies to acquire.

OMB is responsible for ensuring that agencies comply with the standard. OMB's 2005 memorandum to executive branch agencies outlined instructions for implementing HSPD-12 and the new standard. The memorandum specified 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.⁹

- October 27, 2005. For all new employees and contractor personnel, adhere to the identity proofing, registration, card issuance, and maintenance requirements of the first part (PIV-I) of the standard.

⁹In 2007, OMB issued a memorandum clarifying the schedule agencies were given to complete the background investigations on all current employees and contractor personnel and issue personal identity verification credentials.

-
- 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 contractor personnel who have been with the agency for 15 years or less. Issue PIV cards to these employees and contractor personnel 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.¹⁰

In addition, OMB directed that each agency provide certain information on its plans for implementing HSPD-12, including the number of individuals requiring background checks and the dates by which the agency planned to be compliant with PIV-I and PIV-II requirements. OMB required agencies to post quarterly reports beginning on March 1, 2007, on their public websites showing the number of background checks that had been completed and PIV credentials that had been issued. Each quarter, OMB has posted a summary report of the governmentwide implementation status of HSPD-12 on its website. After determining that a number of agencies were going to have difficulties in meeting the original deadlines for card issuance, OMB requested in fiscal year 2008 that agencies confirm that their previous plans were still on target or provide updated plans with revised schedules for meeting the requirements of HSPD-12 and the OMB memoranda.

Other related guidance that OMB issued includes guidance to federal agencies on electronic authentication practices, sample privacy documents for agency use in implementing HSPD-12, a memorandum to agencies about validating and monitoring agency issuance of PIV credentials, guidance on protecting sensitive agency information, a

¹⁰In January 2007, OMB issued another memorandum to the chief information officers that clarified that employees with more than 15 years of service had to have PIV cards by October 27, 2008. In addition, 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.

memorandum to agencies on safeguarding against and responding to a breach of personally identifiable information, and updated instructions to agencies on publicly reporting their HSPD-12 implementation status.

On June 30, 2006, OMB issued a memorandum to agency officials that provided updated guidance for the acquisition of products and services for the implementation of HSPD-12. Specifically, OMB provided acquisition guidance for FIPS 201-compliant commercial products that have passed, among other tests, NIST's conformance tests and GSA's performance and conformance tests. For example, OMB referred agencies to a special item number on GSA's IT Schedule 70 for the acquisition of approved HSPD-12 implementation products and services, noting that all products and services offered under the special item number had been evaluated and determined to be in compliance with governmentwide requirements. When agencies acquire HSPD-12 products and services through acquisition vehicles other than the specified GSA schedule, the OMB memo required them to ensure that only approved products and services were acquired and to ensure compliance with other federal standards and requirements for systems used to implement HSPD-12.

In addition, GSA established a managed service office 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 April 2011, GSA had 90 agency customers with more than 591,000 government employees and contractor personnel to whom cards were issued through shared service providers. In addition, as of April 2011, the Managed Service Office had installed over 385 enrollment stations with 18 agencies actively enrolling employees and issuing PIV cards. While there are several services offered by the office, it is not intended to provide support for all aspects of HSPD-12 implementation. For example, the office 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 and the federal Chief Information Officers (CIO) Council¹¹ 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 April 2011, the group had issued 13 interface specification documents, including a specification for exchanging data between an agency and a shared service provider.

Previously Reported HSPD-12 Implementation Challenges

In February 2006, we reported that agencies faced several challenges in implementing HSPD-12, 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 websites quarterly reports on the number of PIV cards they had issued to their employees, contractor personnel, 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 did not implement this recommendation.

In February 2008, we reported that much work had been accomplished to lay the foundations for implementation of HSPD-12 but that agencies had made limited progress in implementing and using PIV cards.¹³ In addition, we noted that a key factor contributing to agencies' limited progress was that OMB had at the time emphasized the issuance of cards and not the full use of the cards' capabilities. We recommended that OMB establish realistic milestones for full implementation of the infrastructure needed to best use the electronic capabilities of PIV cards in agencies. We also recommended that OMB require agencies to align the acquisition of PIV cards with plans for implementing their technical infrastructure to best use the cards' electronic authentication capabilities. In February 2011, OMB

¹¹The federal CIO Council is the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of federal information resources.

¹²[GAO-06-178](#).

¹³[GAO-08-292](#).

directed agencies to issue implementation policies by March 31, 2011, through which the agencies will require use of the PIV credentials as the common means of authentication for access to agency facilities, networks, and information systems. Agencies were instructed to include the following requirements, among others, in their policies: all new systems under development must be able to use PIV credentials prior to being made operational, existing physical and logical access control systems must be upgraded to use PIV credentials, and agency processes must accept and electronically verify PIV credentials issued by other federal agencies.

OMB and Agencies Have Made Progress but Have Not Yet Fully Implemented Homeland Security Presidential Directive 12

Overall, OMB and federal agencies have made mixed progress in implementing HSPD-12 requirements aimed at establishing a common identification standard for federal employees and contractor personnel. On the one hand, the federal CIO Council, OMB, and NIST have issued guidance to agencies specifying milestones for conducting background investigations and issuing PIV cards as well as requirements for implementing the electronic authentication capabilities of the cards. Also, agencies have made substantial progress in conducting background investigations and issuing PIV cards. However, a few agencies reported that background investigations and card issuance for contractor personnel and “other” staff—defined by OMB as short-term employees (less than 6 months on the job), guest researchers, volunteers, and intermittent, temporary, or seasonal employees—were not as complete. Additionally, agencies have made fair progress in implementing the electronic capabilities of the PIV card for physical access to their facilities. While they have generally begun using PIV cards for access to their headquarters buildings, most have not implemented the same capabilities at their major field office facilities. Further, limited progress has been made in using PIV cards for access to agency information systems. Several agencies have taken steps to acquire and deploy hardware and software allowing users to access agency information systems via PIV cards, but none have fully implemented the capability. Lastly, agencies have made minimal progress in achieving the goal of interoperability among agencies, having generally not established systems and procedures for universally reading and electronically validating PIV cards issued by other federal agencies.

The Federal CIO Council, OMB, and NIST Have Taken Steps to Promote Full Implementation of HSPD-12

While early HSPD-12 guidance from OMB focused on completion of background investigations and issuance of PIV cards, beginning in 2008 the federal CIO Council, OMB, and NIST took actions to more fully address HSPD-12 implementation, including focusing on the use of the electronic capabilities of the cards for physical and logical access control.

In November 2009, the federal CIO Council issued the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance, which established a common framework for agencies to use in planning and executing identity, credential, and access management programs. The roadmap went further than previous guidance in providing guidance to agencies on complete operational scenarios involving HSPD-12 authentication. It also outlined strategies for developing a standardized identity and access management system across the federal government and defined “use cases” and transition milestones to assist agencies in implementing the identity, credential, and access management architecture. For example, the roadmap’s use cases addressed topics such as “Create, Issue, and Maintain PIV Card,” “Grant Physical Access to Employee or Contractor,” and “Grant Visitor or Local Access to Federally-Controlled Facility or Site.” These use cases specified detailed models for agencies to follow in designing processes to carry out these functions.

In May 2008, OMB issued guidance to agencies on preparing or refining plans for incorporating the use of PIV credentials with physical and logical access control systems.¹⁴ The guidance included a checklist of questions for agencies to consider when planning for the use of PIV credentials with physical and logical access control systems. Examples of the questions include:

- Does your agency have a documented plan for incorporating the use of PIV credentials for both physical and logical access control?
- Does your agency have policy, implementing guidance, and a process in place to track progress toward the appropriate use of the PIV credentials?

¹⁴OMB, *Memorandum for Chief Information Officers: Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation* (Washington, D.C.: May 23, 2008).

-
- Does your plan include a process for authorizing the use of other agency PIV credentials to gain access to your facilities and information systems?
 - Has your agency identified all physical access points where you intend to require access using the electronic capabilities of the PIV credentials?
 - Has your agency performed the analyses to identify the changes that must be made to upgrade its systems' capabilities to support use of the electronic capabilities of the PIV credentials for physical access?

Further, in February 2011, OMB issued guidance that reiterated agency responsibilities for complying with HSPD-12 and specified new requirements.¹⁵ OMB required agencies to develop implementation policies by March 31, 2011, through which the full use of PIV credentials for access to federal facilities and information systems would be required. The implementation policies were required to include the following provisions:

- effective immediately, enable the use of PIV credentials in all new systems under development;
- effective as of the beginning of fiscal year 2012, upgrade all existing physical and logical access control systems to use PIV cards before investing in other activities;
- procure all services and products for facility and system access control in accordance with HSPD-12 policy;
- accept and electronically verify PIV credentials issued by other federal agencies; and
- align HSPD-12 implementation plans with the federal CIO Council's Federal Identity, Credential, and Access Management Roadmap.

¹⁵OMB, *Memorandum for the Heads of Executive Departments and Agencies: Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, M-11-11 (Washington, D.C.: Feb. 3, 2011).

OMB's February 2011 guidance was much more explicit than its previous HSPD-12 guidance in requiring agencies to make use of the electronic capabilities of PIV cards. The guidance noted that the majority of the federal workforce, as of December 2010, was in possession of PIV credentials and thus agencies were in a position to aggressively step up their efforts to use the electronic capabilities of the credentials.

Lastly, beginning in fiscal year 2010, OMB required agencies to report detailed security metrics, including PIV card usage status for both logical and physical access, through the Federal Information Security Management Act Cyberscope system, which is designed to capture operational pictures of agency systems and provide insight into agency information security practices.

In 2008, NIST issued guidance on using PIV credentials in physical access control systems.¹⁶ The guidance provided a detailed analysis of threat considerations, PIV authentication mechanisms, and potential use cases, so that agencies would be able to determine what specific physical access control system architectures to implement at their facilities. Specifically, this guidance discusses various PIV card capabilities, so that risk-based assessments can be made and appropriate PIV authentication mechanisms selected to manage physical access to federal government facilities.

Agencies Have Made Substantial Progress in Conducting Background Investigations and Issuing PIV Credentials

FIPS 201 requires agencies to adopt an accredited proofing and registration process that includes, among other things, initiating or completing a background investigation or ensuring that one is on record for all employees and contractor personnel before they are issued PIV cards. The standard requires agencies to adopt an accredited card issuance and maintenance process. Based on this requirement, in August 2005, OMB directed agencies to verify or complete background investigations for all employees, contractor personnel, and other staff seeking access to federal facilities and information systems and issue PIV cards for their use by October 2008. We reported in February 2008 that

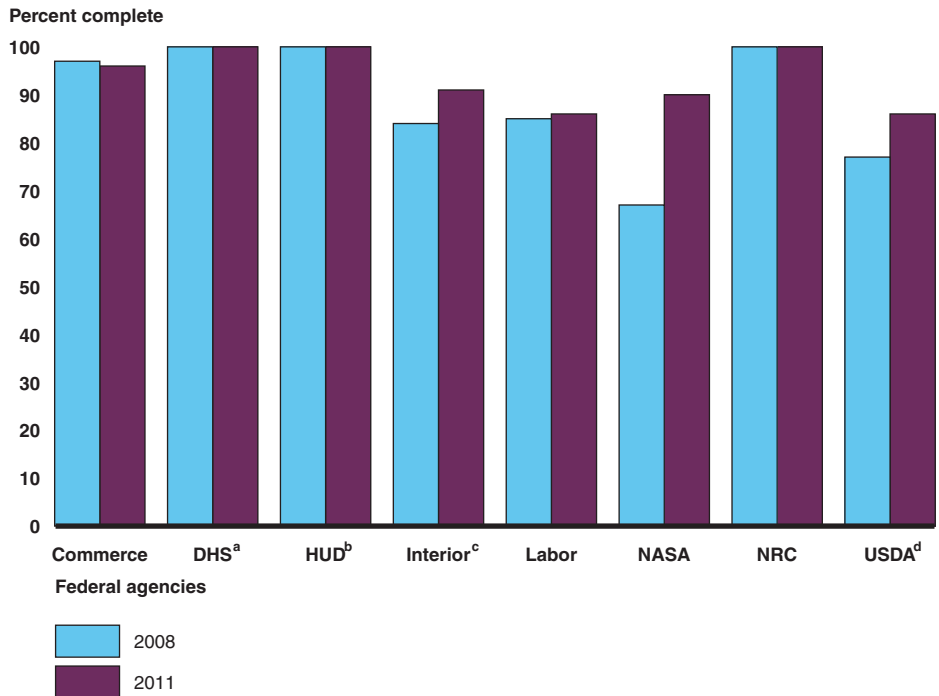
¹⁶NIST, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, Special Publication 800-116 (Gaithersburg, Md.: November 2008).

agencies had generally completed background checks for most of their employees and contractor personnel.¹⁷

Since 2008, agencies have made further progress in completing background investigations for the majority of personnel requiring them. Three of the agencies that we reviewed, DHS, HUD, and NRC, had successfully completed background investigations for all such personnel, including employees and contractor staff. All of the remaining five agencies—Commerce, Interior, Labor, NASA, and USDA—had completed investigative checks for over 85 percent of their employees and contractor staff. Figure 2 shows the eight agencies' progress from 2008 to 2011 in conducting required background investigations for all staff requiring them, such as employees, contractor staff, and other staff.

¹⁷[GAO-08-292](#).

Figure 2: Agencies' Progress in Completing Background Checks from 2008 and 2011



Source: GAO analysis of agency data.

^aAccording to DHS, current employee, contractor personnel, and other staff numbers do not include the U.S. Coast Guard, which will primarily be utilizing the Department of Defense Common Access Card. Also, contractor personnel and other individual numbers represent an estimate of the total number of contractor personnel and other individuals based on estimates provided by components.

^bAccording to HUD officials, as of March 2009, they had completed all required background investigations and fully issued PIV credentials and therefore would not be posting any further updates to the agency's issuance information. However, new background investigations are required on a continuing basis as the agency hires new employees. Officials stated that, as of June 2011, 548 background investigations for new hires had not yet been completed.

^cAccording to Interior, each bureau and office generated a "best estimate" for the total number of contractor personnel and other staff since the department does not maintain a central database for background investigation data and does not have a departmentwide database containing information on all contractor personnel and other types of staff.

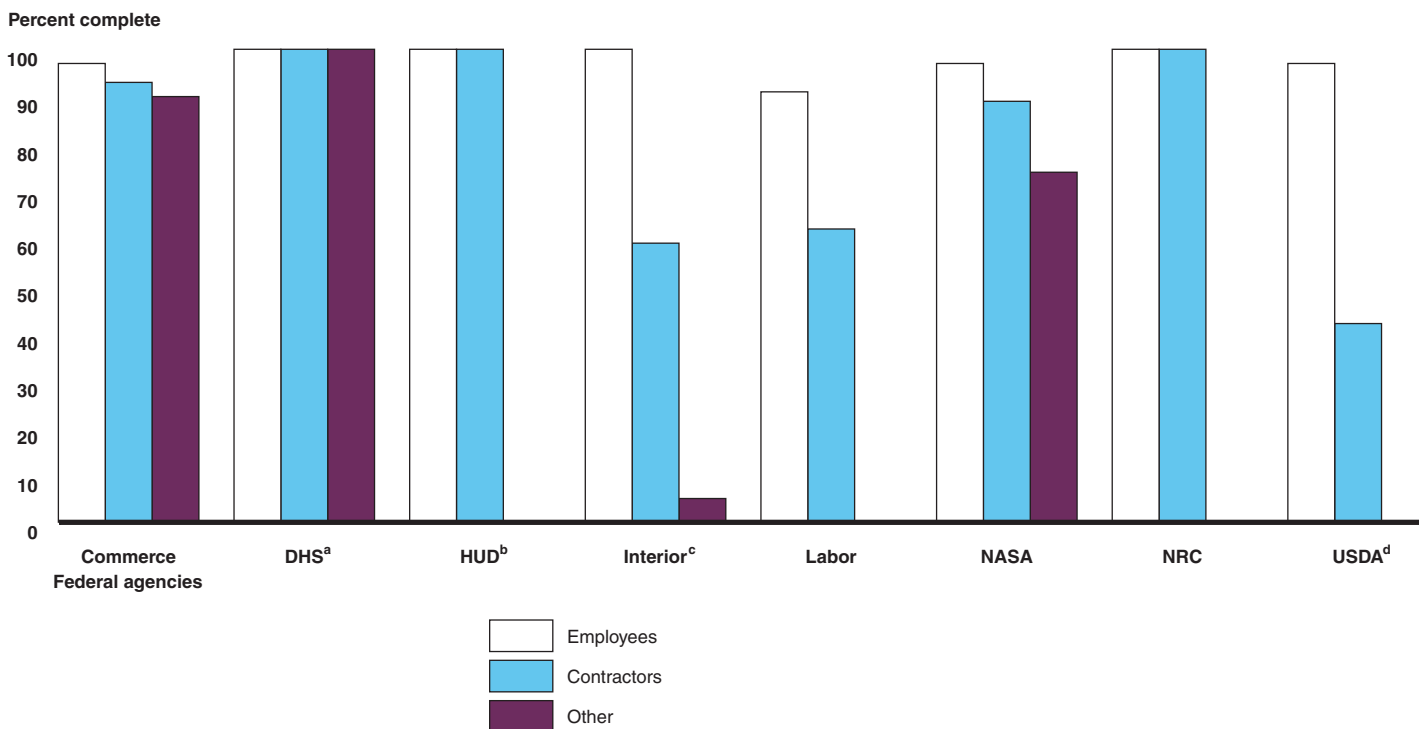
^dAccording to USDA, numbers for background investigations were not provided in its quarterly report for contractor personnel in 2008 and for other staff in 2008 and 2011 because departmentwide data collection was not completed to provide this information.

While agencies have made progress overall in completing background investigations for most of their employees, several agencies still have not completed all required investigations. These agencies reported that background investigations for contractor and other staff were often not as

complete as investigations for employees. According to officials at Interior and Labor, the high turnover rate of these staff is one of the key contributing factors to their inability to maintain completed background investigations for higher percentages of these staff. Likewise, according to a USDA official, a large number of seasonal employees are hired each year, particularly in the firefighting season, and it is difficult to maintain a high percentage of completed background checks for these types of employees.

Figure 3 shows agencies' completion rates of background checks for employees, contractor personnel, and other personnel as of March 2011.

Figure 3: Agencies' Progress in Completing Background Checks by Personnel Groups as of March 2011



Source: GAO analysis of agency reported data.

^aAccording to DHS, current employee, contractor personnel, and other staff numbers do not include the U.S. Coast Guard, which will primarily be utilizing the Department of Defense Common Access Card. Also, contractor personnel and other individual numbers represent an estimate of the total number of contractor personnel and other individuals based on estimates provided by components.

^bAccording to HUD officials, as of March 2009, they had completed all required background investigations and fully issued PIV credentials and therefore would not be posting any further updates to the agency's issuance information. However, new background investigations are required on a continuing basis as the agency hires new employees. Officials stated that, as of June 2011, 548 background investigations for new hires had not yet been completed.

^cAccording to Interior, each bureau and office generated a "best estimate" for the total number of contractor personnel and other staff since the department does not maintain a central database for background investigation data and does not have a departmentwide database containing information on all contractor personnel and other types of staff.

^dAccording to USDA, numbers for background investigations were not provided in its quarterly report for contractor personnel in 2008 and for other staff in 2008 and 2011 because departmentwide data collection was not completed to provide this information.

Since 2008, agencies have also made substantial progress in issuing PIV cards to employees and other personnel requiring them. Of the eight agencies we reviewed, two (HUD and NRC) have issued PIV card credentials to their entire workforce, and two (Labor and NASA) have issued PIV cards to at least 93 percent of their personnel requiring such credentials. The other four agencies (Commerce, DHS, Interior, and USDA) have issued cards to between 69 percent and 80 percent of their personnel requiring credentials.

According to Commerce officials, the department's issuance numbers were low (69 percent) specifically because its U.S. Patent and Trademark Office (USPTO) had been slow to issue PIV credentials. Unlike the rest of Commerce, USPTO did not rely on GSA's Managed Services Office for card issuance. According to these officials, USPTO was given permission to use its existing PKI infrastructure to issue PIV cards, which has taken extra time. Commerce officials said they expected to complete issuance of PIV cards to all staff requiring cards by May 2012.

DHS had issued PIV cards to about 80 percent of its workforce as of March 31, 2011. In response to OMB's call for implementation plans from agencies in 2008, DHS submitted a plan that foresaw completion of card issuance by December 31, 2010. However, DHS did not meet the revised deadline. The department's Office of Inspector General reported in January 2010 that the slow progress was the result of weak program management, including insufficient funding and resources, and a change in implementation strategy from a component-by-component to a centralized approach.¹⁸ At the time of our review, the department was

¹⁸Department of Homeland Security, Office of Inspector General, *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12*, OIG-10-40 (Washington D.C.: Jan. 25, 2010).

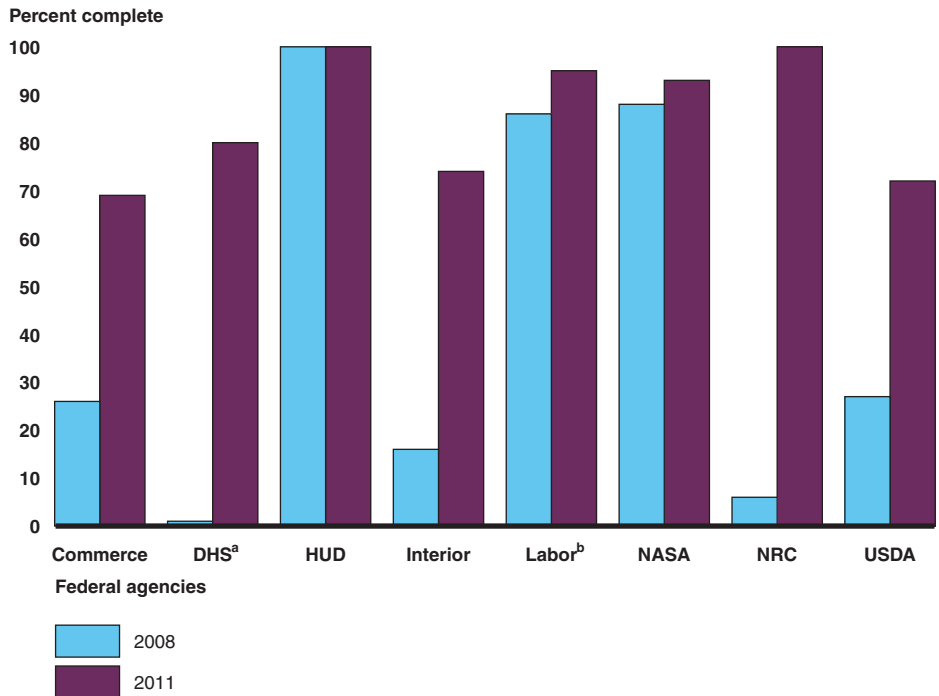
working to meet a new deadline of September 30, 2011, to complete issuance of PIV cards.

Interior officials stated that the department's issuance numbers were low (74 percent) due to difficulties in issuing cards to personnel in remote field offices. According to these officials, 400 to 500 locations have been identified to be serviced by "mobile" PIV credentialing stations. Before credentialing can be done at these locations, local staff must be trained and certified in performing registration duties. Interior officials stated that they intended to establish target completion dates for issuing credentials at these locations but had not yet done so.

USDA officials said their department had previously focused on issuing PIV cards to employees and that many of its component agencies had not established roles and responsibilities for issuing PIV cards to contractor and other staff until fiscal year 2011. According to these officials, the proper management structure is now in place and PIV cards are to be issued to the majority of contractor and other staff by the end of fiscal year 2011.

Figure 4 shows agencies' progress in issuing PIV cards to all staff requiring cards, such as employees, contractor staff, and other staff, between 2008 and 2011.

Figure 4: Agencies' Progress in Issuing PIV Cards from 2008 and 2011



Source: GAO analysis of agency data.

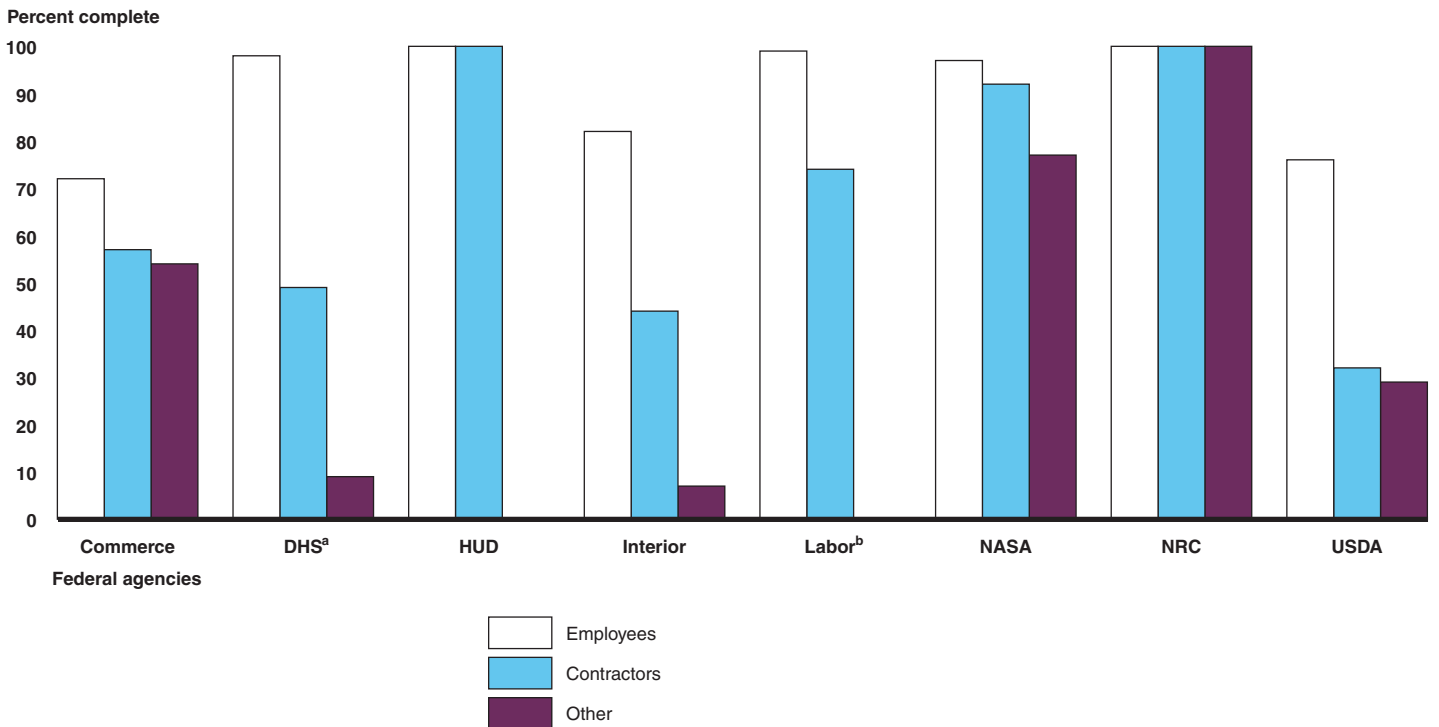
^aAccording to DHS, current employee, contractor personnel, and other staff numbers do not include the U.S. Coast Guard, which will primarily be utilizing the Department of Defense Common Access Card. Also, contractor personnel and other individual numbers represent an estimate of the total number of contractor personnel and other individuals based on estimates provided by components.

^bAccording to Labor, it could not accurately report the number of contractor staff who have been issued PIV cards. While the department developed a reporting methodology for adjusting totals downward in order to produce more conservative measures of the count of contractors issued PIV cards, we are not assured that this estimate is correct. Labor officials stated that they are in the process of developing a new system that will more accurately track issuance of credentials to contractor staff.

Contractor and other staff, such as temporary and seasonal employees, are a substantial portion of federal agency and department personnel and often require access to agency facilities and information systems. However, agencies have not made as much progress issuing PIV cards to their contractor and other staff as they have for their employees. Based on data provided by agencies, the eight agencies we reviewed issued PIV credentials to a total of 91 percent of their employees, 69 percent of their contractor personnel, and 35 percent of their other personnel as of March 2011.

Among the eight agencies reviewed, three (HUD, NASA, and NRC) have issued PIV credentials to at least 90 percent of their contractor personnel. The remaining five have lower issuance numbers varying between 32 percent and 74 percent. According to agency officials, the constant turnover of contractor and other personnel makes it more difficult to ensure that cards are issued to all such staff needing them. Figure 5 illustrates agencies' progress in issuing PIV cards to employees, contractor personnel, and other personnel as of March 2011.

Figure 5: Agencies' Progress in Issuing PIV Cards by Personnel Groups as of March 2011



Source: GAO analysis of agency reported data.

^aAccording to DHS, current employee, contractor personnel, and other staff numbers do not include the U.S. Coast Guard, which will primarily be utilizing the Department of Defense Common Access Card. Also, contractor personnel and other individual numbers represent an estimate of the total number of contractor personnel and other individuals based on estimates provided by components.

^bAccording to Labor, it could not accurately report the number of contractor staff who have been issued PIV cards. While the department developed a reporting methodology for adjusting totals downward in order to produce more conservative measures of the count of contractors issued PIV cards, we are not assured that this estimate is correct. Labor officials stated that they are in the process of developing a new system that will more accurately track issuance of credentials to contractor staff.

Agencies Have Made Fair Progress in Implementing the Electronic Capabilities of the PIV Credentials for Physical Access to Federal Facilities

HSPD-12 states that agencies shall require the use of the PIV credentials for access to federal facilities to the maximum extent practicable. OMB's 2005 guidance directed agencies to make risk-based determinations about the type of authentication mechanisms to deploy at their facilities but specified "minimal reliance" on visual authentication as a sole means of authenticating PIV credentials. FIPS 201 and NIST guidance on using PIV credentials in physical access systems also both state that visual authentication provides only a basic level of assurance regarding the identity of a PIV cardholder. OMB's 2011 guidance required agencies to step up their efforts to use the electronic capabilities of PIV credentials as the common means of authentication for access to agency facilities. We reported in February 2008 that agencies generally had not been using the cards' electronic authentication capabilities for physical access.

Agencies have made fair progress in using the electronic capabilities of the PIV cards for physical access to their facilities.¹⁹ For example, two of the eight agencies we reviewed (NASA and NRC) reported using the electronic capabilities of the PIV cards for physical access to both their headquarters and field office facilities. Specifically, NRC was using electronic verification of the PIV card's CHUID combined with visual authentication by a guard as the predominant electronic authentication method at its facilities. NASA officials reported that their agency was using electronic CHUID verification combined with visual authentication as the predominant access control method at its headquarters facility and for access to buildings within major field locations.

Four agencies (DHS, HUD, Interior, and Labor) reported that while they had begun utilizing the electronic capabilities of the PIV card at their headquarters, they had not yet begun using them at all of their major field office facilities. According to DHS officials, the agency has conducted an assessment of all its facilities in the National Capitol region to determine what method of authentication was being used for physical access and to develop a strategy to implement PIV-based electronic authentication at each facility. DHS officials stated that approximately 70 percent of these facilities utilize the electronic capabilities of the PIV card for physical access. The same officials stated that they plan to complete a similar assessment of DHS facilities outside of the National Capital region by the

¹⁹All eight agencies reported that they had conducted risk assessments of their major facilities or had such assessments conducted by the DHS Federal Protective Service to determine appropriate assurance levels for these facilities.

fourth quarter of fiscal year 2011. Additionally, DHS officials stated that a new departmentwide implementation strategy will be completed by the second quarter of fiscal year 2012.

HUD officials stated that their previous strategy had been to install PIV-related upgrades to physical access control systems in conjunction with other scheduled renovations at each of their field offices. As of March 2011, HUD officials stated that 13 of its 83 field offices had upgraded physical security systems. In December 2008, HUD submitted a plan to OMB establishing fiscal year 2013 as the completion date for the upgrades to the majority of its field offices and fiscal year 2015 for its smallest field offices. According to a HUD official, they are currently planning to issue PIV credentials to all field offices by the end of fiscal year 2014, pending availability of funds.

Interior officials stated that they were using the electronic capabilities of the PIV card at several, but not all, of their major field offices. According to Interior officials, in response to OMB's guidance to step up efforts to use the PIV credentials for access to agency facilities, they established a new Identity, Credential, and Access Management Program Office and plan to convene a working group of representatives from each departmental bureau to develop plans for modernizing the physical access control infrastructure. No time frame has been established for completing these plans.

Labor officials stated that they were using the electronic capabilities of the PIV card at 2 of their 10 regional field offices and were assessing the remaining offices to determine whether upgrades to the physical security systems were needed to enable PIV-based electronic authentication. The assessment is expected to be completed by the end of fiscal year 2012, after which necessary upgrades are to be implemented based on priority and the availability of funding.

The remaining two agencies (Commerce and USDA) were not using PIV-based electronic authentication at their headquarters facilities or the majority of their other major facilities. A Commerce official stated that major upgrades were still needed to physical access control systems throughout the department to support HSPD-12 requirements, including replacing card readers and upgrading software. Previously the department had focused on card issuance and had not developed plans for card usage. In September 2010, a contractor completed an assessment of the status of physical access systems at the department's major facilities to determine what steps were needed to develop a

departmentwide HSPD-12-compliant system,²⁰ but specific implementation plans for such a system have not yet been developed.

Regarding PIV-enabled access to their headquarters buildings, USDA officials stated that the department was in the process of purchasing card-reader-equipped turnstiles, but that they were unsure when they would be installed because funding had not been obtained. In addition, officials stated that 130 of the department's 250 major field facilities had begun using PIV credentials for access control through the departmentwide physical security system. For the remaining locations, USDA's component agencies had not yet committed to replacing their hardware and integrating their software with the departmentwide system. USDA officials stated that use of PIV cards for physical access previously had been considered a low priority within the agency, and, as a result, progress had been slow.

Agencies Have Made Limited Progress in Implementing the Electronic Capabilities of the PIV Credentials for Logical Access to Federal Information Systems

HSPD-12 requires agencies to use PIV credentials for access to federal information systems. FIPS 201 identifies different methods of electronic authentication that are available via PIV cards for logical access and the respective assurance levels associated with each method. OMB's 2011 guidance required agencies to step up their efforts to use the electronic capabilities of PIV credentials as the common means of authentication for access to agency information systems. We reported in February 2008 that select agencies had generally not been using the cards for logical access.

Since then, agencies have made limited progress in utilizing the electronic capabilities of the PIV credential for access to systems. Five of the agencies we reviewed (NASA, HUD, Interior, NRC, and USDA) had taken steps to acquire and deploy hardware and software allowing substantial numbers of users to access agency systems via PIV-based authentication, but none of them had fully implemented the capability or were requiring use of PIV cards as a primary means of authenticating users.

²⁰Diebold Inc., *NOAA PACS Migration & Modernization Initiative HSPD12 Compliance Final Review Draft* (Chesapeake, Va.: Sept. 25, 2010).

For example, NASA officials reported that 83 percent of the agency's Windows desktops were equipped with PIV card readers and that the agency's network and 622 separate software applications had all been configured for authentication using PIV cards.²¹ Nevertheless, users still could log on to NASA systems using a combination of username and password. Agency officials estimated that only 10 percent of users were using PIV cards for authentication. According to NASA officials, users reported in a survey that they did not see the benefits of using the PIV card to access the agency network because they still had to maintain their network password to access other software applications or to access the network from another device. NASA officials stated that they were planning to upgrade additional applications to exclusively use PIV cards for logical access, but they did not have time frames for the completion of this activity.

A HUD official stated that the department had enabled the electronic capabilities of the PIV card for access to its network, but nevertheless, users still could log onto the HUD network using a combination of username and password. According to the same official, HUD had deployed card readers on most of its agency computers to enable use of PIV cards for access to the network. An official stated that HUD is currently developing a strategy that will define milestones for departmentwide implementation of PIV-enabled logical access and identify the necessary technology to make full use of the PIV card for logical access. A HUD official stated that HUD had not established a date for full implementation of the electronic capabilities of the PIV card for logical access.

According to a department official, Interior does not currently utilize PIV cards to access the department's network within departmental offices but has begun utilizing the capability for remote access. An official reported that approximately 17,000 users require remote access to Interior systems on a regular basis. At the time of our review, between 8,000 and 9,000 of these users had been issued laptop computers that were configured to use PIV cards for authentication. Interior officials estimated that approximately 3,000 of those individuals were actually using PIV-based authentication on a regular basis. The Office of the Chief

²¹NASA officials also stated that a number of employees within the agency utilize Apple Mac desktops, which they said cannot be enabled to use the PIV card for logical access.

Information Officer issued a policy mandating the use of the PIV card for all remote access to the department's network by December 2010, but that goal had not yet been reached. Officials reported they were beginning to plan for the implementation of PIV-enabled local access to the department's network from workstations within its offices but had not yet set a milestone for completing that activity.

NRC officials stated that they had acquired hardware and software to enable PIV-based logical access for all of their employees and planned to have them deployed to all workstations by the end of 2011. The agency had a small pilot of approximately 50 employees from headquarters and five regional offices under way to test PIV-based authentication to the agency's network. The pilot was scheduled to be completed in the fourth quarter of fiscal year 2011, and the agency planned to achieve full implementation of PIV-based logical access by December 31, 2011.

A department official stated that USDA had PIV-enabled all of its user hardware (both laptop and desktop systems) as well as 423 web-based software applications, including remote access to agency systems. This same official believed that some of USDA's 90,000 users were using their PIV cards to access agency systems and applications, but they did not have an estimate of the number. USDA also had not established a target date for requiring use of the PIV card for access to agency systems and applications.

The other three agencies (Commerce, DHS, and Labor) had made less progress. While all were developing plans or had limited trial deployments under way, none of these agencies had deployed hardware and software that would enable PIV-based authentication to systems and networks for substantial numbers of their users.

According to a department official, Commerce was not using PIV cards for access to its systems. The department formed a working group with representatives from each component to investigate logical access solutions for the department. According to officials, one component, NIST, has enabled approximately 150 workstations to accept PIV cards for logical access, but NIST users were not regularly using the capability. Commerce's identity management plan indicates that it intends to achieve full internal implementation of PIV-based logical access in fiscal year 2013.

DHS officials stated they began planning in May 2011 for PIV-based systems access across the department in response to OMB's February

2011 guidance. They added that the initial planning effort is expected to be completed in the fourth quarter of fiscal year 2012. At the time of our review, a pilot project was under way at DHS headquarters whereby approximately 1,000 employees were using PIV cards to access the agency's network. DHS officials said they planned to expand this pilot project to all DHS headquarters offices by the end of the first quarter of fiscal year 2012. According to officials, the department is developing plans to require headquarters personnel to use PIV cards for access to the department's network but has not established a completion date.

Labor officials stated they were conducting a pilot in the Office of the Assistant Secretary for Administration and Management to test the use of PIV cards to access the agency's network. According to these officials, Labor plans to enable PIV-based network access for a larger population of users beginning in fiscal year 2012; however, it may need to purchase replacement hardware and software to achieve this goal.

Agencies Have Made Minimal Progress in Establishing Interoperability with Other Federal Departments and Agencies

Interoperability refers to the ability of two or more systems or components to exchange information and use the information exchanged. The FIPS 201 standard and related NIST guidance established specifications to ensure that PIV cards and systems developed by different vendors would be interoperable from a technical standpoint. NIST and GSA also established testing programs to ensure that PIV products and services conformed to these standards. These efforts have helped to ensure that card readers and associated software systems are able to read and process the data on any PIV card, including cards produced by different vendors for other federal agencies. In addition, Federal Identity, Credential, and Access Management implementation guidance issued by the federal CIO Council provides examples that illustrate how agencies could implement procedures to accept and electronically validate PIV credentials from other agencies. Moreover, OMB guidance requires agencies to take steps to establish processes and procedures for accepting and validating PIV cards issued by other agencies and ensure that agencies' systems are capable of validating cards electronically.

Several of the agencies we reviewed have taken steps to accept PIV cards issued by other agencies in limited circumstances. For example, officials from Interior and USDA stated they were working together to develop policies and procedures for enrolling PIV credentials from both agencies in their existing physical and logical access systems at key sites, such as the National Interagency Fire Center, which is staffed by employees of Interior and USDA's Forest Service. According to a USDA

official, the PIV cards of Interior employees can be manually enrolled in USDA's physical access control system; however, when those employees stop working at USDA sites, their card registration information must be manually deleted from the USDA system. Similarly, according to a DHS official, the Federal Emergency Management Agency (FEMA) has developed procedures for manually enrolling the PIV credentials of other federal officials who need access to certain FEMA-controlled facilities, such as the National Emergency Center.

These examples demonstrate the feasibility of establishing PIV card interoperability among agencies but also show the limitations of implementing "manual" processes that do not include electronic validation of credentials. Specifically, each of these cases is limited in scope and requires officials to take extra steps to ensure the validity of cards issued by other agencies.

Only one of the agencies we reviewed had plans to establish a system capable of universally reading and electronically validating PIV cards issued by all other federal agencies. Specifically, NASA officials stated they were developing a formal credential registration process that would enable them to enroll the PIV credentials of external federal personnel seeking access to NASA facilities and information systems into the agency's centralized identity management system. NASA officials estimated this project would be completed by the end of fiscal year 2011.

Agencies Face Obstacles in Fully Implementing Homeland Security Presidential Directive 12

Agencies reported that their mixed progress in issuing PIV credentials and using them for electronic authentication of individuals accessing federal facilities and information systems can be attributed to several major management and technical obstacles. These include logistical difficulties associated with issuing PIV cards to personnel in remote field locations, as well as tracking and then revoking cards issued to contractor personnel, the lack of priority attention and adequate resources being focused on implementing PIV-enabled physical access at all major facilities, the absence of a full suite of procedures for requiring the use of PIV cards for logical access, and the lack of procedures and assurances for interoperability among federal agencies.

Several Agencies Reported Logistical Difficulties Associated with Issuing Credentials to Employees in Remote Locations

OMB's August 2005 guidance specifies that HSPD-12 credentials are to be issued to all employees and contractor personnel in executive branch agencies who require long-term access to federally controlled facilities or information systems. The guidance instructed agencies to make risk-based decisions on whether to issue PIV cards to specific types of individuals, such as short-term employees (less than 6 months on the job), guest researchers, volunteers, and intermittent or temporary employees. All employees and contractor personnel requiring long-term access to federal facilities and systems, regardless of physical location, were instructed to be issued PIV cards.

Officials from four agencies (DHS, Interior, Labor, and USDA) stated that challenges in providing PIV cards to personnel in remote field office locations had hindered their ability to complete PIV-card issuance requirements set forth by OMB and in the FIPS 201 standard. These agencies all have large numbers of employees and contractor staff in field office locations, some of which are remote and difficult to access.

The PIV-card issuance process requires at least one visit to an office equipped with a credentialing station, so that fingerprints can be taken and individuals can be enrolled in the agency's identity management system. Credentialing stations were originally deployed to few field locations, thus requiring staff at remote locations to make potentially expensive and time-consuming trips to obtain PIV cards.

DHS, Interior, and Labor officials indicated that the limited number of credentialing centers and the travel costs to access those centers made it logistically difficult to meet card issuance targets. While these logistical issues have caused challenges in issuing cards to remote field staff, actions can be taken to minimize the expense and disruption of issuing cards to these individuals. Officials from Interior, Labor, and USDA stated they had used "mobile" PIV credentialing stations provided by GSA's Managed Services Office or other GSA-approved solutions to issue PIV cards to field staff. According to a USDA official, these inexpensive, portable stations, part of GSA's USAccess Program, offer enhanced flexibility to enroll employees and activate PIV cards at field locations.

In addition to logistical concerns, USDA officials stated they faced challenges in determining whether staff in the "other" category—specifically seasonal and temporary employees, such as firefighters and summer volunteers—should receive credentials and what processes should be established for handling them. According to these officials, the department's tally of "other" staff receiving PIV credentials was low in part

due to this challenge. However, these staff are not necessarily required to obtain PIV credentials. OMB guidance instructed agencies to make risk-based determinations on whether to issue PIV cards to staff in the “other” category. Once a determination is made not to issue PIV cards to a specific group, those individuals are not included in the total population needing cards and thus should not be a factor in calculating an agency’s progress in card issuance.

Until agencies take steps to address logistical challenges associated with card issuance and make risk-based determinations about how to handle “other” staff, they are likely to continue to be unable to reach HSPD-12’s objectives of issuing PIV cards to all personnel requiring access to federal facilities and systems.

Several Agencies Have Not Established Effective Mechanisms for Tracking Issuance and Revocation of PIV Cards for Contractor Personnel

Contractor and temporary staff may be responsible for carrying out a wide range of mission-critical tasks requiring access to agency facilities and information systems. The FIPS 201 standard requires agencies to implement an identity management system with the ability to track the status of PIV credentials throughout their lifecycle, including activation and issuance, as well as suspension, revocation, and destruction. Additionally, the standard requires that, upon the issuance of credentials, agencies keep track of all active, lost, stolen, and expired cards. To do so, agencies must establish a card registry to document and monitor all cards issued to employees and contractor staff.

Officials from three agencies (Commerce, DHS, and HUD) identified difficulties they faced in monitoring and tracking contractor personnel, especially when contracts begin and end, as a reason for not fully complying with HSPD-12 requirements for background investigations and/or PIV card issuance and revocation. According to agency officials, the inability to track when contractor personnel leave prevents them from ensuring that all PIV credentials are returned upon termination of a contract.

Commerce officials stated they had initiated a project to develop and deploy a system to improve tracking of PIV card issuance to contractor personnel. The system is being designed to automatically trigger revocation of PIV credentials as part of the exit process for departing contractor personnel. However, Commerce officials did not provide an estimated date for implementation of the new system.

DHS officials stated they had experienced problems tracking contractor personnel and documenting when their credentials were scheduled to be revoked. Officials stated it was difficult to monitor contractor projects, which may often be extended, and ensure that their systems were updated to reflect these changes. The officials stated that they had developed revisions to their existing procedures to better ensure that PIV cards issued to contractor personnel are revoked, returned to the agency, and accounted for. However, they did not provide an estimated date for implementation of the revised procedures.

HUD officials stated that although they had issued cards to all of their contractor personnel, they had deferred addressing issues with monitoring the status of contractor PIV cards. They stated that control procedures had not been put into place to ensure that PIV cards were promptly revoked for departing contractor staff, and officials acknowledged that some contractor staff had left the agency without returning PIV cards issued to them. HUD officials did not know how often this had occurred. According to these officials, the problem could be addressed by including all contractor staff in the identity management system HUD uses for PIV cards issued to employees and by establishing controls to ensure that cards are returned upon departure of all staff. However, they did not provide an estimated date for implementing these changes.

At the time of our review, Commerce, DHS, and HUD had not set time frames for implementing planned improvements. Until they develop and implement procedures for effectively controlling the issuance of PIV cards to contractor personnel and revoking expired contractor cards, these agencies could be at risk that unauthorized individuals could access their facilities and information systems if other compensating controls are not in place.

Several Agencies Have Not Put a Priority on Implementing the Electronic Capabilities of the PIV Credentials for Physical Access to Their Major Facilities

HSPD-12 required the use of the PIV credential for access to federal facilities. OMB's 2005 guidance instructed agencies to make risk-based determinations about the type of authentication mechanisms to utilize at their facilities and specified "minimal reliance" on visual authentication as a sole means of authenticating PIV credentials. OMB's February 2011 guidance required agencies to increase usage of the electronic capabilities of PIV credentials as the common means of authentication for access to agency facilities.

Officials from six agencies (Commerce, DHS, HUD, Interior, Labor, and USDA) indicated that implementing PIV-enabled physical access had not been a priority at their agencies and that resources had not been committed to fully implementing the electronic capabilities of the PIV-card at all of their facilities as required by HSPD-12.

Even though 6 years have passed since OMB first issued guidance on implementation of HSPD-12, Commerce, DHS, and Interior have not yet developed specific plans for fully implementing PIV-enabled physical access throughout their departments. At Commerce, a contractor-led study of the existing physical access control systems at major facilities and the infrastructure needed to develop a departmentwide HSPD-12-compliant system was completed in September 2010. However, Commerce has not yet developed a plan for implementing such a system within the department. DHS officials stated that they still had not yet determined what physical access systems were in place throughout their agencies and what investment would be needed to upgrade or replace the systems to achieve a departmentwide HSPD-12-compliant system. According to a 2010 report by the DHS Office of Inspector General, the department had not made the implementation of an effective HSPD-12 program a priority and did not have a plan for enhancing the department's physical access controls.²² DHS officials stated that they had recently formed a working group dedicated to physical access. The group had begun determining what systems were in place throughout the department and planned to report quarterly on its progress to OMB. Although Interior issued an official policy in 2009 requiring use of PIV credentials for physical access, the department does not have a plan in place to implement the policy. Interior officials stated that they plan to convene a working group of representatives from each departmental bureau to develop plans for modernizing their physical access control infrastructure.

The other three agencies—HUD, Labor, and USDA—had developed plans for PIV-enabled physical access but had not obtained funds to pay for implementation or had delayed implementation to reduce investment costs. Officials from HUD, for example, had planned to not implement PIV-enabled access at field locations until each location was scheduled

²²Department of Homeland Security, Office of Inspector General, *Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12* (Washington, D.C.: Jan. 25, 2010).

for renovations, to reduce costs. The agency planned to re-examine that strategy based on OMB's February 2011 guidance. Labor officials stated that they previously had been planning to enable PIV-based access at their field locations in fiscal year 2012 but were planning to develop revised milestones for those implementations due to budget constraints. Officials at USDA stated that they were in the process of purchasing equipment for PIV-enabled physical access.

Use of PIV credentials for physical access is unlikely to progress at these six agencies until greater priority is placed on implementation of PIV-based physical access control systems. Until Commerce, DHS, and Interior develop specific implementation plans for their major facilities, including identifying necessary infrastructure upgrades and time frames for deployment, they are unlikely to reach HSPD-12's objective of using of the PIV credential to enhance control over access to federal facilities. HUD, Labor, and USDA are also unlikely to reach that objective until they place greater priority on funding PIV-enabled physical access at their major facilities.

Agencies Have Not Established a Full Suite of Procedures for Using PIV Cards as the Primary Means for Access to Their Networks and Information Systems

HSPD-12 requires agencies to use PIV credentials for access to federal information systems to the maximum extent practicable. OMB's 2005 guidance required agencies to prioritize implementation based on authentication risk assessments required by previous OMB and NIST guidance. Additionally, OMB's February 2011 guidance required agencies to step up their efforts to use the electronic capabilities of PIV credentials as the common means of authentication for access to agency information systems.

Officials from four agencies (HUD, NRC, NASA, and USDA) reported that various technical issues hindered using PIV cards as the primary means of access to agency networks and systems. One technical issue that agencies reported was not having backup procedures to authenticate employees who did not possess a PIV card. Officials from HUD, NASA, and USDA stated that, although they had deployed software and hardware to enable PIV-based access to systems and networks, they were not using the cards as the primary means of authentication to agency systems because they had not established backup procedures to authenticate employees who did not possess a PIV card. According to these officials, the issue of how to accommodate personnel without PIV cards was a major obstacle to requiring the use of PIV cards for access to networks and systems.

There are several reasons why staff might not have a PIV card when trying to access agency systems. Individuals could have left the card at another location or lost the card. The card may have been damaged and made inoperable. Also, some staff may not have any cards issued to them. Short-term employees (less than 6 months on the job), guest researchers, volunteers, and intermittent or temporary employees, for example, may not be required to have PIV cards but may still need access to agency networks and systems.

Agency officials reported that they were working on solutions to this problem. Officials at HUD and USDA, for example, stated that they were working on developing standard procedures to address these circumstances. NASA officials stated they were participating in a governmentwide team tasked with drafting guidance for issuing smart cards to people who do not qualify for PIV cards but need access to agency facilities and systems. Until HUD, NASA, and USDA develop and implement procedures for providing temporary logical access to their systems as a backup mechanism, they are unlikely to reach HSPD-12's objective of using of the PIV credential to enhance control over access to federal systems.

Other technical issues reported by agency officials included adapting to the requirement that workstations be locked when PIV cards are removed and using hardware that was not compatible with PIV cards. Specifically, NRC and USDA officials stated that governmentwide security policies requiring workstations to be locked when removing the PIV card makes using the PIV card for logical access in a laboratory setting difficult because employees routinely need access to multiple computers at the same time. If they were required to use the PIV card for logical access, they would be unable to remain logged in to multiple computers. Additionally, NASA officials stated that many of its employees utilize Apple Mac workstations or mobile devices to carry out their work responsibilities. The same officials noted that the PIV card is incompatible with these devices; therefore, employees must continue to use their username and password for access to the NASA network when using these devices.

Officials from the other four agencies (Commerce, DHS, and Interior, and Labor) indicated that implementing PIV-enabled logical access had not been a priority at their agencies and that resources had not been committed to fully implementing the electronic capabilities of the PIV-card for access to their networks and systems. Commerce, DHS, Interior, and Labor officials, for example, stated that their agencies had not yet

determined what logical access systems were currently in place throughout their agencies and what investment would be needed to upgrade or replace them to achieve a departmentwide HSPD-12-compliant system. They also stated that funding constraints had hindered implementing PIV-based logical access in a timelier manner. Commerce, DHS, Interior, and Labor are unlikely to fulfill the objectives of the HSPD-12 program until greater management priority is placed on implementation of PIV-based logical access control systems.

Agencies Have Not Established Procedures and Assurances to Implement Access Control Systems That Accept PIV Cards from Other Agencies

One of the primary goals of the HSPD-12 program 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.²³ To overcome this limitation, HSPD-12 directed ID cards to have standard features and means for authentication. Further, guidance from OMB required agencies to have access control processes that accept and electronically verify PIV credentials issued by other federal agencies.

Nevertheless, agencies have made minimal progress in implementing access control systems that can accept and validate PIV cards issued by other agencies. Several of the agencies we reviewed, including Commerce, HUD, and Labor, had not devoted resources or management attention to achieving cross-agency interoperability, according to agency officials. This limited progress reflects, in part, the low priority OMB initially put on achieving cross-agency interoperability. OMB guidance initially focused on card issuance and set performance measures keyed exclusively to progress in that area. According to an OMB official, specific interoperability requirements were not established until November 2009, when the office directed agencies to develop detailed policies for aligning their identity, credential, and access management activities with the Federal Identity, Credential and Access Management Roadmap and Implementation Guidance. As part of their policies, agencies were required to enable relevant applications to accept PIV cards from other executive branch agencies for authentication.

In addition to a lack of systems and processes in place at agencies to electronically validate PIV cards issued by other agencies, there are also

²³[GAO-06-178](#).

no processes in place to ensure that credentials issued by agencies are trustworthy and should be accepted by other agencies as a basis for granting access to their facilities and systems. Processes have not been developed to establish trustworthiness by validating the certification processes at agencies. HSPD-12 guidance allows agencies to independently develop FIPS 201-compliant credentialing systems, and NIST issued guidance in 2005 for certifying and accrediting organizations that issue PIV credentials.²⁴ However, according to GSA officials, the approach envisioned in the NIST guidance, which relies on self-certification, has not been adequate to establish trust. The primary reason self-certification has not worked is that it does not include a provision for independent validation, such as through the use of third-party audits. OMB officials agreed that a third-party validation process would be useful in establishing trust. Until such a process is in place, agencies may be reluctant to authorize access to their facilities and systems based on PIV credentials issued by other agencies.

Until agencies develop implementation plans for accepting and electronically verifying external agency credentials and a process is established to provide assurance that external PIV credentials are trustworthy, progress in achieving HSPD-12's goal of governmentwide interoperability for PIV credentials will likely remain limited.

Conclusions

Agencies have made substantial progress in issuing PIV cards to employees and contractor personnel and have begun using the electronic capabilities of the cards for physical and logical access but have made less progress in using the credentials for access to federal facilities and information systems. They face a variety of obstacles in fully issuing the credentials and making better use of their electronic capabilities. For example, several have experienced difficulties in issuing credentials to remote and "other" staff and in ensuring that expired credentials are promptly revoked. Six agencies were not using the electronic capabilities of the credentials for access to all of their major facilities because doing so was not a priority in terms of management commitment and resources. None of the eight agencies had fully implemented logical access to networks and systems using PIV credentials, half because of technical

²⁴NIST, *Guidelines for the Certification and Accreditation of PIV Card Issuers*, Special Publication 800-79-1.

challenges and half because it was not a priority to do so. Delaying implementation of HSPD-12 means that the benefits of enhanced security that HSPD-12 is designed to provide are also being delayed. Without taking steps to resolve technical problems and setting a higher priority on implementation, agencies are not likely to make substantially better progress in addressing these obstacles.

Establishing interoperability among agencies has also been a challenge. Agencies have established policies and procedures for accepting credentials from other agencies only in limited circumstances, in part because OMB only began requiring that agency systems accept credentials from other agencies in 2009. Interoperability among agencies has also been hindered by the lack of third-party audit mechanisms to establish the trustworthiness of agency implementations of HSPD-12. Until such mechanisms are in place, agencies are likely to continue to make slow progress in achieving interoperability.

Recommendations for Executive Action

To address challenges in conducting background investigations, issuing PIV cards, and using the cards for physical and logical access, we are making 23 recommendations to the eight departments and agencies we reviewed in our report to help ensure they are meeting the HSPD-12 program's objectives. Appendix IV contains these recommendations.

To address the challenge of promoting the interoperability of PIV cards across agencies by ensuring that agency HSPD-12 systems are trustworthy, we recommend that the Director of OMB require the establishment of a certification process, such as through audits by third parties, for validating agency implementations of PIV credentialing systems.

Agency Comments and Our Evaluation

We sent draft copies of this report to the eight agencies covered by our review, as well as to OMB and GSA. We received written responses from Commerce, DHS, HUD, Interior, Labor, NASA, and NRC. These comments are reprinted in appendices V through XI. We received comments via e-mail from OMB, USDA, and GSA.

Of the nine agencies to which we made recommendations, six (Commerce, DHS, Interior, Labor, NASA, and NRC) concurred with our recommendations. In cases where these agencies also provided technical comments, we have addressed them in the final report as appropriate. DHS, Interior, Labor, and NASA also provided information regarding

specific actions they have taken or plan on taking that address portions of our recommendations. Further, DHS, Labor, and NASA provided estimated timelines for completion of actions that would address our recommendations.

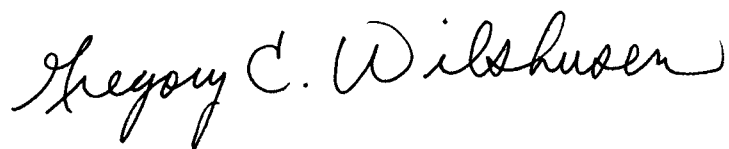
HUD's Acting Chief Human Capital Officer did not state whether the department concurred with our recommendations. However, she provided information about actions the department is taking to address each of them. For example, she provided updated information on HUD's schedule for implementing PIV-based physical access control at its field locations and for requiring staff to use their PIV cards to gain access to agency systems. We have updated the final report with this information as appropriate.

The two remaining agencies (OMB and USDA) did not comment on the recommendations addressed to them. However, OMB and USDA provided technical comments on the draft report, which were addressed in the final report as appropriate.

We also received technical comments via e-mail from GSA. These comments have also been incorporated into the final report as appropriate.

We are sending copies of this report to other interested congressional committees; the Secretaries of the Departments of Agriculture, Commerce, Homeland Security, Housing and Urban Development, the Interior, and Labor; the Administrators of the General Services Administration and National Aeronautics and Space Administration; the Chairman of the Nuclear Regulatory Commission; and the Director of the Office of Management and Budget. The report also is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of the report. Key contributors to the report are listed in appendix XII.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large, prominent 'G' and 'W'.

Gregory C. Wilshusen
Director, Information Security Issues

List of Congressional Requesters

The Honorable Joseph I. Lieberman
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
Chairman
Subcommittee on Federal Financial Management,
Government Information, Federal Services,
and International Security
Committee on Homeland Security
and Governmental Affairs
United States Senate

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine the progress that selected agencies have made in implementing the requirements of Homeland Security Presidential Directive 12 (HSPD-12) and (2) identify obstacles agencies face in implementing the requirements of HSPD-12. We conducted our audit work at the same eight agencies we reviewed for our last report.¹ They were the Departments of Agriculture, Commerce, the Interior, Homeland Security (DHS), Housing and Urban Development (HUD), and Labor; the National Aeronautics and Space Administration (NASA); and the Nuclear Regulatory Commission (NRC). These agencies were chosen in 2008 based on the fact that they were each in different stages of implementing smart card programs and were using different strategies for implementing HSPD-12. Our selection included agencies that were acquiring personal identity verification (PIV) card systems through the General Services Administration's (GSA) Managed Services Office as well as agencies that were acquiring PIV card systems independently.

To address our first objective, we reviewed HSPD-12, Federal Information Processing Standards (FIPS) 201, related National Institute of Standards and Technology (NIST) special publications, and guidance from the Office of Management and Budget (OMB) to determine what progress agencies should be making in completing background checks, issuing PIV cards, using PIV cards for physical and logical access, and achieving interoperability with other federal agencies. We analyzed agencies' quarterly status reports to determine the actual progress they had made in each of these areas and compared it with governmentwide guidance, as well as the results from our 2008 report. In order to assess the reliability of the data collected from the eight agencies' quarterly status reports specific to background investigations and PIV card issuance, we submitted questions to the agencies and reviewed agency documentation. In some cases, as we noted where applicable, the data included in the reports were based on the agencies' best estimates. We determined the data were sufficiently reliable for determining overall agency progress in the areas of background investigations and PIV card issuance. To assess progress in the use of PIV credentials for physical and logical access, we reviewed agency documentation such as HSPD-12 implementation plans and policies and discussed progress with agency officials. Additionally, we reviewed previous GAO and agency inspector general reports.

¹[GAO-08-292](#).

To address our second objective, we interviewed officials from the selected agencies to obtain information on obstacles they faced in implementing HSPD-12 requirements, including difficulties in completing background checks, issuing PIV cards, using PIV cards for physical and logical access, and achieving interoperability with other federal agencies. We analyzed the obstacles that were identified to determine whether they were consistent across the agencies in our sample and whether they had been raised or addressed in our previous reviews. We also assessed OMB, GSA, NIST, and federal Chief Information Officers (CIO) Council documentation to determine the extent to which these obstacles could be addressed within the framework of existing guidance. Finally, we interviewed program officials from OMB and GSA who had been involved in supporting implementation of HSPD-12 across the government to discuss actions they had taken to assist agencies in implementing HSPD-12 and to validate the implementation obstacles reported by agency officials.

We conducted this performance audit at Commerce, DHS, GSA, HUD, Interior, Labor, NASA, NRC, OMB, and USDA in the Washington, D.C., area from October 2010 to September 2011 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.

Appendix II: Requirements and Components of PIV-II

The requirements of PIV-II include the following:

- specifications for the components of the PIV system that employees and contractor personnel will interact with, such as PIV cards, card and biometric readers, and personal identification number (PIN) input devices;
- security specifications for the card issuance and management provisions;
- a suite of authentication mechanisms supported by the PIV card and requirements for a set of graduated levels of identity assurances;
- specifications for the physical characteristics of PIV cards, including requirements for both contact and contactless interfaces and the ability to pass certain durability tests; and
- mandatory information that is to appear on the front and back of the cards, such as a photograph, cardholder name, card serial number, and issuer identification.

There are many components of a PIV-II system, including the following:

- enrollment stations—used by the issuing agency to obtain the applicant’s information, including digital images of fingerprints and a digital photograph.
- an ID management system—stores and manages cardholder information, including the status of assigned credentials.
- card issuance stations—issue PIV cards to applicants. Prior to releasing a PIV card to the applicant, the issuer first matches the applicant’s fingerprint to the fingerprint on the PIV card. Once a match has been verified, the applicant is issued the card.
- card management system—manages life-cycle maintenance tasks associated with the credentials, such as “unlocking” the PIV cards during issuance or updating a PIN number or digital certificate on the card.
- a physical access control system—permits or denies a user access to a building or room. This system may use a variety of authentication

mechanisms, ranging from visual inspection by a guard to fingerprint scanning. Once the user has been authenticated and access has been authorized, the physical access control system grants entry to the user.

- logical access control system—permits or denies a user access to information and systems. This system may employ a variety of authentication methods, such as requiring users to enter a password or perform a fingerprint scan.
- public key infrastructure (PKI)—allows for electronic verification of the status of the digital certificates contained on the PIV card. The status of the PIV card—whether it is valid, revoked, or expired—is verified by the card management system.

Appendix III: Selected NIST Guidance

NIST has issued several special publications (SP) providing supplemental guidance on various aspects of the FIPS 201 standard. Selected special publications are summarized in this appendix.

**NIST SP 800-73-3,
Interfaces for
Personal Identity
Verification, February
2010**

SP 800-73-3 is a companion document to FIPS 201 that specifies the technical aspects of retrieving and using the identity credentials stored in a PIV card's memory. This publication is divided into four parts and specifies detailed requirements for the interface between a smart card and other PIV systems. The publication aims to promote interoperability among PIV systems across the federal government by constraining vendors' interpretation of FIPS 201.

**NIST SP 800-76-1,
Biometric Data
Specification for
Personal Identity
Verification, January
2007**

SP 800-76-1 outlines technical acquisition and formatting specifications for the biometric credentials of the PIV system, including the PIV card.

**NIST SP 800-78-3,
Cryptographic
Algorithms and Key
Sizes for Personal
Identity Verification,
December 2010**

SP 800-78-3 outlines the cryptographic mechanism and objects that employ cryptography as specified in FIPS 201. This publication also describes the cryptographic requirements for keys and authentication information stored on the PIV card, status information generated by PKI Certification Authorities, and management of information stored on the PIV card. This publication also identifies PIV card infrastructure components that support issuance and management.

**NIST SP 800-79-1,
Guidelines for the
Accreditation of
Personal Identity
Verification Card
Issuers, June 2008**

SP 800-79-1 describes the guidelines that are to be used by federal departments and agencies to accredit the capability and reliability of PIV card issuers they use to perform PIV card services, such as identity proofing, applicant registration, and card issuance. The new guidelines are based on emergent service models (in-house, leased, shared, etc.), lessons learned in past accreditations, and the directives in OMB memorandums. The publication also describes an assessment model that includes conformance testing, certification, and accreditation. This document provides examples of PIV organization management structures, an objective set of controls for PIV card issuers, an assessment and accreditation methodology that assesses the capability and reliability of a PIV card issuer based on these controls, and sample accreditation decision letters.

**NIST SP 800-85A-2,
PIV Card Application
and Middleware
Interface Test
Guidelines, July 2010**

SP 800-85A-2 outlines a suite of tests to validate a software developer's PIV middleware¹ and card applications to determine whether they conform to the requirements specified in SP 800-73-3. This publication also includes detailed test assertions² that provide the procedures to guide the tester in executing and managing the tests. This document is intended to allow (1) software developers to develop PIV middleware and card applications that can be tested against the interface requirements specified in SP 800-73-3; (2) software developers to develop tests that they can perform internally for their PIV middleware and card applications during the development phase; and (3) certified and accredited test laboratories to develop tests that include the test suites specified in this document and that can be used to test the PIV middleware and card applications for conformance to SP 800-73-3.

**NIST SP 800-85B, PIV
Data Model Test
Guidelines, July 2006**

SP 800-85B outlines a suite of tests to validate a developer's PIV data elements and components to determine whether they conform to the requirements specified in SP 800-73, SP 800-76, and SP 800-78. This publication also includes detailed test assertions that provide the procedures to guide the tester in executing and managing the tests. This

¹Middleware is software that allows software applications running on separate computer systems to communicate and exchange data. In this case, middleware allows external software applications to interact with applications on a smart card.

²Test assertions are statements of behavior, action, or condition that can be measured or tested.

document is intended to allow (1) developers of PIV components to develop modules that can be tested against the requirements specified in SP 800-73-1, SP 800-76, and SP 800-78; (2) developers of PIV components to develop tests that they can perform internally for their PIV components during the development phase; and (3) accredited test laboratories to develop tests that include the test suites specified in this document and that can be used to test the PIV components for conformance to SP 800-73-1, SP 800-76, and SP 800-78.

**NIST SP 800-87
Revision 1 - 2008,
Codes for
Identification of
Federal and
Federally-Assisted
Organizations, April
2008**

SP 800-87 Revision 1 - 2008 provides the organizational codes necessary to establish the Federal Agency Smart Credential Number that is required to be included in the FIPS 201 Card Holder Unique ID (CHUID). SP 800-87 is a companion document to FIPS 201. Appendix A lists the updated agency codes for the identification of federal and federally assisted organizations to be used in the PIV CHUID.

**NIST SP 800-96, PIV
Card to Reader
Interoperability
Guidelines,
September 2006**

SP 800-96 provides requirements for PIV card readers in the area of performance and communications characteristics to foster interoperability. It also outlines requirements for the contact and contactless card readers for both physical and logical access control systems.

**NIST SP 800-104, A
Scheme for PIV Visual
Card Topography,
June 2007**

SP 800-104 provides additional information on the PIV card color-coding for designating employee affiliation. The recommendations in this document complement FIPS 201 in order to increase reliability when visual verification of PIV cards is implemented.

**NIST SP 800-116, A
Recommendation for
the Use of PIV
Credentials in
Physical Access
Control Systems
(PACS), November
2008**

SP 800-116 provides best practice guidelines for integrating the PIV card with the physical access control systems (PACS) that authenticate the cardholders at federal facilities. Specifically, this publication discusses various PIV card capabilities, so that risk-based assessments can be made and appropriate PIV authentication mechanisms selected to manage physical access to federal government facilities. This document also proposes a PIV implementation maturity model to measure the progress of agencies' PIV implementations and recommends an overall strategy for agency implementation of PIV authentication mechanisms within PACS systems.

Appendix IV: Recommendations to Departments and Agencies

Department of Agriculture

To ensure that PIV credentials are issued only to employees and contractor staff requiring them, we recommend that the Secretary of Agriculture take steps to identify which staff in the “other” category should receive PIV cards and establish procedures for handling such cases.

To meet the HSPD-12 program’s objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of Agriculture take the following three actions:

- Ensure that the department’s plans for PIV-enabled physical access at major facilities are implemented in a timely manner.
- Require staff with PIV cards to use them to access systems and networks and develop and implement procedures for providing temporary access to staff who do not have PIV cards.
- Develop and implement procedures to allow employees who need to access multiple computers simultaneously to use the PIV card to access each computer.

Department of Commerce

To ensure that PIV cards do not remain in the possession of staff whose employment or contract with the federal government is over, we recommend that the Secretary of Commerce establish controls, in addition to time frames for implementing a new tracking system, to ensure that PIV cards are revoked in a timely fashion.

To meet the HSPD-12 program’s objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of Commerce take the following two actions:

- Develop specific implementation plans for enabling PIV-based access to the department’s major facilities, including time frames for deployment.
- Ensure that plans for PIV-enabled logical access to the department’s systems and networks are implemented in a timely manner.

Department of Homeland Security

To ensure that PIV credentials are issued to all employees and contractor staff requiring them, we recommend that the Secretary of Homeland Security make use of portable credentialing systems, such as mobile activation stations, to economically issue PIV credentials to staff in remote locations.

To ensure that PIV cards do not remain in the possession of staff whose employment or contract with the federal government is over, we recommend that the Secretary of Homeland Security establish specific time frames for implementing planned revisions to the department's tracking procedures, to ensure that PIV cards are revoked in a timely fashion.

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of Homeland Security take the following two actions:

- Develop specific implementation plans for enabling PIV-based access to the department's major facilities, including identifying necessary infrastructure upgrades and timeframes for deployment.
- Ensure that plans for PIV-enabled logical access to the department's systems and networks are implemented in a timely manner.

Department of Housing and Urban Development

To ensure that PIV cards do not remain in the possession of staff whose employment or contract with the federal government is over, we recommend that the Secretary of Housing and Urban Development develop and implement control procedures to ensure that PIV cards are revoked in a timely fashion.

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of Housing and Urban Development take the following two actions:

- Ensure that the department's plans for PIV-enabled physical access at major facilities are implemented in a timely manner.
- Require staff with PIV cards to use them to access systems and networks and develop and implement procedures for providing temporary access to staff who do not have PIV cards.

Department of the Interior

To ensure that PIV credentials are issued to all employees and contractor staff requiring them, we recommend that the Secretary of the Interior make greater use of portable credentialing systems, such as mobile activation stations, to economically issue PIV credentials to staff in remote locations.

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of the Interior take the following two actions:

- Develop specific implementation plans for enabling PIV-based access to the department's major facilities, including identifying necessary infrastructure upgrades and time frames for deployment.
- Ensure that plans for PIV-enabled logical access to Interior's systems and networks are implemented in a timely manner.

Department of Labor

To ensure that PIV credentials are issued to all employees and contractor staff requiring them, we recommend that the Secretary of Labor make greater use of portable credentialing systems, such as mobile activation stations, to economically issue PIV credentials to staff in remote locations.

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal facilities, networks, and systems, we recommend that the Secretary of Labor take the following two actions:

- Ensure that the department's plans for PIV-enabled physical access at major facilities are implemented in a timely manner.
- Ensure that plans for PIV-enabled logical access to Labor's systems and networks are implemented in a timely manner.

National Aeronautics and Space Administration

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal networks and systems, we recommend that the Administrator of NASA take the following two actions:

- Require staff with PIV cards to use them to access systems and networks and develop and implement procedures for providing temporary access to staff who do not have PIV cards.
- Develop and implement procedures for PIV-based logical access when using Apple Mac and mobile devices that do not rely on direct interfaces with PIV cards, which may be impractical.

Nuclear Regulatory Commission

To meet the HSPD-12 program's objectives of using the electronic capabilities of PIV cards for access to federal networks and systems, we recommend that the Chairman of the NRC develop and implement procedures to allow staff who need to access multiple computers simultaneously to use the PIV card to access each computer.

Appendix V: Comments from the Department of Commerce



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

August 22, 2011

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to offer the Department of Commerce's comments on recommendations outlined by the U.S. Government Accountability Office (GAO) draft report entitled "Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards" (GAO-11-751).

We generally concur with the report's recommendations regarding the Department's findings for Homeland Security Presidential Directive-12's program objectives of using the electronic capabilities of personal identity verification (PIV) cards for access to Federal facilities, networks, and systems. We also concur with the report's recommendations on implementation of specific plans to enable PIV-based physical and logical access.

We welcome any further communication with GAO regarding its conclusions and look forward to receiving the final report. Please contact Earl Neal at (202) 482-1148 if you have any questions regarding this response.

Sincerely,

A handwritten signature in black ink that reads "Rebecca Blank".

Rebecca M. Blank
Acting Secretary of Commerce

Enclosure

Appendix VI: Comments from the Department of Homeland Security

Office of the Chief Security Officer
U.S. Department of Homeland
Security
Washington, DC 20528



**Homeland
Security**

August 19, 2011

Gregory C. Wilshusen
Director, Information Security Issues
441 G Street, NW
U.S. Government Accountability Office
Washington, DC 20548

Re: Draft Report GAO 11-751, "PERSONAL ID VERIFICATION: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards"

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's positive acknowledgement that DHS has nearly completed issuing personal identity verification (PIV) cards to its entire workforce. DHS leadership is committed to effectively implementing the Department's PIV card program and achieving the enhanced security envisioned by Homeland Security Presidential Directive 12.

The draft report contained four recommendations directed at DHS, with which DHS concurs. Specifically, GAO recommended that the Secretary of Homeland Security:

Recommendation 1: Make use of portable credentialing systems, such as mobile activation stations, to economically issue PIV credentials to staff in remote locations.

Response: Concur. DHS Identity Management Division (IMD) and the Office of the Chief Information Officer (OCIO) are currently evaluating portable credentialing systems and mobile activation stations to accommodate staff in remote locations. The Department will procure additional mobile activation stations, as evaluation warrants and funding becomes available, during fiscal years 2012–2015.

Recommendation 2: Establish specific timeframes for implementing planned revisions to the Department's tracking procedures, to ensure that PIV cards are revoked in a timely fashion.

Response: Concur. On July 27, 2011, IMD issued new procedures for revoking and destroying PIV cards for DHS employees and contractors. Further, on August 5, 2011, a change was made to the Identity Management System which allows the PIV expiration to be set to a specific date. This ensures that a PIV Card for a contractor or a person working for DHS on a work visa can be programmed to expire on a date that is earlier than the 3-year default period. These new procedures will ensure that PIV cards are revoked in a timely fashion.

Recommendation 3: Develop specific implementation plans for enabling PIV-based access to the Department's major facilities, including identifying necessary infrastructure upgrades and timeframes for deployment.

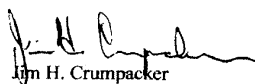
Response: Concur. DHS IMD established an integrated physical security project team to develop comprehensive Department-wide plans for PIV-enabled physical security systems across the enterprise. DHS anticipates having an enterprise strategy by December 31, 2011.

Recommendation 4: Ensure that plans for PIV-enabled logical access to the Department's systems and networks are implemented in a timely manner.

Response: Concur. DHS OCIO established an integrated project team to develop comprehensive, Department-wide plans for PIV-enabling DHS systems, applications, and networks. DHS anticipates having a DHS enterprise plan by December 31, 2011, for PIV enabling DHS IT networks in accordance with OMB M-11-11 memorandum, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors," dated February 3, 2011.

Again, thank you for the opportunity to review and comment on this draft report. We look forward to working with you on future Homeland Security related issues.

Sincerely,



John H. Crumpacker
Director
Departmental GAO/OIG Liaison Office

Appendix VII: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF HUMAN CAPITAL OFFICER

AUG 26 2011

Ms. Marisol Cruz
Senior Analyst
U. S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

RE: GAO Draft Report Entitled Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards (GAO-11-751)

Dear Ms. Cruz:

The Office of the Chief Human Capital Officer (OCHCO) has completed the review of the draft report entitled Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards (GAO-11-751).

HUD appreciates the opportunity to respond to your draft report. Following are the three recommendations for our Department and the corresponding proposed corrective action plans.

Recommendation #1: To ensure that PIV cards do not remain in the possession of staff whose employment or contract with the Federal Government is over, we recommend that the Secretary of Housing and Urban Development develop and implement control procedures to ensure that PIV cards are revoked in a timely fashion.

HUD has strong out-processing controls for departing employees that require the return of HUD employee PIV cards. Out-processing controls for contractors can be improved.

Corrective Action Plan #1: OCHCO has created a draft out-processing form for departing contractors. By initiating this process, the agency will be able to ensure all network and systems accounts, identification cards, and other government property is returned to the designated official in a timely manner. Enclosed are draft copies of Clearance for Separation of Contractors, HUD-58-C (Enclosure A), and Out-Processing for Contractors instruction sheet (Enclosure B).

Recommendation #2: Ensure that the Department's plan for PIV-enabled physical access at major facilities is implemented in a timely manner.

Corrective Action Plan #2: HUD plans to upgrade all 87 field facilities by FY 2015. The schedule and cost for installing the remaining PIV-enabled physical security access (PACS) to HUD field offices and facilities is enclosed (Enclosure C). HUD informed OMB, per our HSPD-12 Implementation Plan Update (December 2008), that it would complete the installation of all

www.hud.gov

espanol.hud.gov

**Appendix VII: Comments from the Department
of Housing and Urban Development**

Physical Access Control Systems by the end of FY 2015. This completion date is reinforced by HUD's current implementation plan, currently in HUD clearance and pending Secretarial approval, per the request of OMB memorandum M-11-11, dated February 3, 2011.

HUD's proposed schedule, pending funding or other changes in office relocations, has all field offices and facilities becoming completed in FY 2014 with the majority of offices being completed in FY 2012 and FY 2013. The majority of this funding requirement, a total of \$3.05 million, was requested in the Office of Human Capital Field Support's annual budget for FY 2012 and FY 2013. The schedule calls for the following office completions:

- Completed to date – 17
- FY 2011 – 6
- FY 2012 – 34
- FY 2013 – 25
- FY 2014 – 5

Enclosed for your review is a spreadsheet of all field facilities (Enclosure C).

Recommendation #3: Require staff with PIV cards to use them to access systems and networks and develop and implement procedures for providing temporary access to staff that do not have PIV cards.

Corrective Action Plan #3: In January 2012, HUD will begin the phased implementation to require staff use of their PIV card to gain logical access. By that time, HUD will have drafted and implemented the procedures for providing temporary access to staff that do not have PIV cards.

If you have questions regarding the Department's submission, please contact Guy Wilson, Director, Internal Controls and Risk Management. Mr. Wilson can be reached at 202.402.3792.

Sincerely,



Karen Newton Cole
Acting Chief Human Capital Officer

Enclosures

Appendix VIII: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240



AUG 18 2011

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, *PERSONAL ID VERIFICATION: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards* (GAO-11-751).

The draft report states that federal agencies including the Department of the Interior (DOI) have made progress toward, but have not fully implemented, Homeland Security Presidential Directive 12 (HSPD-12) issued in 2004.

The DOI generally concurs with the recommendations issued by GAO. Some general comments in response to the recommendations are enclosed.

If you have any questions, please contact Judy Snoich, the DOI Identity, Credential and Access Management (ICAM) Program Manager at (703) 648-5623.

Sincerely,

Rhea Suh
Assistant Secretary
Policy, Management and Budget

Enclosure

Department of the Interior
Comments in response to GAO Draft report on *PERSONAL ID VERIFICATION: Agencies*
Should Set a Higher Priority on Using the Capabilities of Standardized
Identification Cards (GAO-11-751)

Recommendation 1: To ensure that PIV credentials are issued to all employees and contractor staff requiring them, we recommend that the Secretary of the Interior make greater use of portable credentialing systems, such as mobile activations, to economically issue PIV credentials to staff in remote locations.

Interior concurs with this recommendation to complete issuance of credentials through the use of Light Activation Systems at our remote office locations, and initiation of a pilot to utilize mobile Light Credentialing Stations. These efforts are underway today and will facilitate credential issuance to the remaining 8,000 employees.

Recommendation 2: Develop specific implementation plans for enabling PIV-based access to the department's major facilities, including identifying necessary infrastructure upgrades and timeframes for deployment.

Interior concurs with the recommendation to develop specific implementation plans for the major facilities that align with efforts to upgrade or replace existing Physical Access Control Systems and can be accommodated within budgets. These plans will address the method of authentication required by the Department of Homeland Security Interagency Security Committee (ISC) Standard, and identify a strategy to implement PIV-based electronic authentication where required.

Recommendation 3: Ensure that plans for PIV-enabled logical access to Interior's systems and networks are implemented in a timely manner.

Interior concurs that the policy requiring use of PIV credentials for remote access through the Virtual Private Network (VPN) to Interior's internal networks should be fully implemented. Interior is implementing an Information Technology Transformation that includes implementation of this policy.

Appendix IX: Comments from the Department of Labor

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210



AUG 19 2011

Mr. Gregory C. Wilshusen
Director
Information Security Issues
Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

This letter is provided in response to the draft report GAO-11-751, *Personal ID Verification – Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards*, dated September 2011. We take seriously our responsibilities to verify the identities of our workforce, and to provide secure access to Department of Labor (DOL) facilities and systems.

Overall, the draft report provides a fair depiction of the Department's efforts to meet Office of Management and Budget (OMB) memorandum, M-05-24 "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors." DOL met or substantially met all interim issuance objectives since October 2005, and currently is underway with implementing use of the personal identity verification (PIV) card for physical and logical access. We recognize the technology and budget challenges, but remain committed in prioritizing and attaining the goals of HSPD-12.

Recommendation #1: Make greater use of portable credentialing systems, such as mobile activation stations, to economically issue PIV credentials to staff in remote locations.

DOL response: The Department implemented a mobile-issuance program beginning in 2008 that continues to enable issuance of PIV credentials to staff in remote locations. With new technology improvements that can securely enable PIV issuance and activation, the Department would augment its current mobile capabilities, based on availability of funds.

Recommendation #2: Ensure that the department's plans for PIV-enabled physical access at major facilities are implemented in a timely manner.

DOL response: The Department agrees with the recommendation. During FY12, DOL plans to establish policies to expand use of PIV-enabled physical access control systems at major facilities. Plans will incorporate revisions from NIST SP800-73-3 specifications.

Recommendation #3: Ensure that plans for PIV-enabled logical access to Labor's systems and networks are implemented in a timely manner.

DOL response: DOL has addressed this recommendation during FY11 and continuing in FY12, as part of implementing an identity and access management (IAM) solution. IAM allows DOL users to use the PIV card for access to networks and systems. Implementation of this capability will be contingent on the budget situation, and other factors such as the Department's IT modernization program and development of new agency applications and services.

Thank you again for the opportunity to comment on the draft report. If you have any questions or you require further discussion about our comments, please have your staff contact Mr. Richard Lewis, DOL HSPD-12 Program Manager, at Lewis.Richard@dol.gov or 202-693-4149.

Sincerely,



T. Michael Kerr
Assistant Secretary for Administration and Management,
Chief Information Officer

Appendix X: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001



August 16, 2011

Reply to Attn of: Office of Protective Services

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the GAO draft report entitled, "Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards" (GAO-11-751).

In the draft report, GAO makes two recommendations to ensure that NASA meets the Homeland Security Presidential Directive (HSPD) 12 program's objectives of using the electronic capabilities of Personal Identity Verification (PIV) cards for access to Federal networks and systems. Specifically, GAO recommends that the NASA Administrator:

Recommendation 1: Require staff with PIV cards to use them to access systems and networks and develop and implement procedures for providing temporary access to staff who do not have PIV cards.

Management Response: Concur. The requirement for using PIV cards as the primary means of access to systems and networks is outlined in NASA's Identity, Credential, and Access Management (ICAM) Implementation Plan. Today, persons holding PIV credentials may access their Windows desktops and systems integrated into the ICAM infrastructure. Implementation of the priorities outlined in the ICAM Implementation Plan will result in NASA being able to require staff with PIV cards to use them to access systems and networks and will provide the capability for providing temporary access to staff who do not have PIV cards.

Planned Corrective Action Date: Fiscal Year 2014, contingent on funding availability.

Recommendation 2: Develop and implement procedures for PIV-based logical access when using Apple Mac and mobile devices that do not rely on direct interfaces with PIV cards, which may be impractical.

Management Response: Concur. NASA is currently investigating options for upgrading its infrastructure to support PIV-based logical access using Apple Mac and mobile devices, which may or may not rely on direct use of PIV cards. The requirement for Apple Mac devices is included in the ICAM Implementation Plan as a priority.

Planned Corrective Action Date: Fiscal Year 2014, contingent on funding availability.

If you have any questions or require additional information, please contact Mark Dodd either by telephone at (202) 358-1255 or via e-mail at mark.r.dodd@nasa.gov.

Sincerely,



Jack Forsythe
Assistant Administrator
Office of Protective Services

Appendix XI: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

August 19, 2011

Mr. Gregory C. Wilshusen, Director
Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

This letter responds to your July 27, 2011, request for comments on the U.S. Government Accountability Office (GAO) draft report entitled "Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards" (GAO-11-751). The U.S. Nuclear Regulatory Commission (NRC) agrees with the report and the recommendation for NRC to develop and implement procedures to allow staff who need to access multiple computers simultaneously to use their Personal Identity Verification card to access each computer.

Thank you for the opportunity to comment on the GAO draft report.

Sincerely,

A handwritten signature in black ink that reads "R. W. Borchardt".

R. W. Borchardt
Executive Director
for Operations

Appendix XII: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contact named above, John de Ferrari, Assistant Director; Sher'rie Bacon; Marisol Cruz; Neil Doherty; Matthew Grote; Lee McCracken; Constantine Papanastasiou; David Plocher; and Maria Stattel made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

