

February 2008

ELECTRONIC GOVERNMENT

Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards





Highlights of [GAO-08-292](#), a report to congressional committees

Why GAO Did This Study

Many forms of identification (ID) that federal employees and contractors use to access government-controlled buildings and information systems can be easily forged, stolen, or altered to allow unauthorized access. In an effort to increase the quality and security of federal ID and credentialing practices, the President issued Homeland Security Presidential Directive 12 (HSPD-12) in August 2004, requiring the establishment of a governmentwide standard for secure and reliable forms of ID. The resulting standard is referred to as the personal identity verification (PIV) card. GAO was asked to determine the progress selected agencies have made in (1) implementing the capabilities of the PIV cards to enhance security and (2) achieving interoperability with other agencies. To address these objectives, GAO selected eight agencies that have a range of experience in implementing smart card-based ID systems and analyzed what actions the agencies have taken to implement PIV cards.

What GAO Recommends

GAO is making recommendations to OMB, including setting realistic milestones for implementation of the electronic authentication capabilities and requiring that each agency develop detailed plans regarding the extent to which it will implement these capabilities. OMB provided comments on GAO's recommendations but did not specifically agree or disagree with any of them.

To view the full product, including the scope and methodology, click on [GAO-08-292](#). For more information, contact Linda D. Koontz at (202) 512-6240 or koontzl@gao.gov.

ELECTRONIC GOVERNMENT

Additional OMB Leadership Needed to Optimize Use of New Federal Employee Identification Cards

What GAO Found

Much work has been accomplished to lay the foundations for implementation of HSPD-12, a major governmentwide undertaking. However, agencies have made limited progress in implementing and using PIV cards. The eight agencies GAO reviewed—including the Departments of Agriculture, Commerce, Homeland Security, Housing and Urban Development, the Interior, and Labor; the Nuclear Regulatory Commission; and the National Aeronautics and Space Administration—have generally completed background checks on most of their employees and contractors and established basic infrastructure, such as purchasing card readers. However, none of them met the Office of Management and Budget's (OMB) goal of issuing PIV cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that have been issued, most agencies have not been using the electronic authentication capabilities on the cards and have not developed implementation plans for those capabilities. In certain cases, products are not available to support those authentication mechanisms. A key contributing factor for why agencies have made limited progress is that OMB, which is tasked with ensuring that federal agencies successfully implement HSPD-12, has emphasized issuance of cards, rather than full use of the cards' capabilities. Specifically, OMB has set milestones that focus narrowly on having agencies acquire and issue cards in the near term, regardless of when the electronic authentication capabilities of the cards may be used. Furthermore, agencies anticipate having to make substantial financial investments to implement HSPD-12, since PIV cards are considerably more expensive than traditional ID cards. However, OMB has not considered HSPD-12 implementation to be a major new investment and thus has not required agencies to prepare detailed plans regarding how, when, and the extent to which they will implement the electronic authentication mechanisms available through the cards. Without implementing the cards' electronic authentication capabilities, agencies will continue to purchase costly PIV cards to be used in the same way as the much cheaper, traditional ID cards they are replacing. Until OMB revises its approach to focus on the full use of the capabilities of the new PIV cards, HSPD-12's objectives of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

While steps have been taken to enable future interoperability, progress has been limited in making current systems interoperate, partly because key procedures and specifications have not yet been developed to enable electronic cross-agency authentication of cardholders. According to General Services Administration officials, they have taken the initial steps to develop guidance to help enable the exchange of identity information across agencies, and they plan to complete and issue it by September 2008. Such guidance should help enable agencies to establish cross-agency interoperability—a primary goal of HSPD-12.

Contents

Letter		1
	Results in Brief	3
	Background	6
	Limited Progress Has Been Made in Implementing PIV Cards and in Using Their Full Capabilities	19
	Efforts Are Under Way to Address the Limited Progress Made in Achieving Interoperability to Enable Cross-Agency Authentication of Cardholders	28
	Conclusions	29
	Recommendations for Executive Action	30
	Agency Comments and Our Evaluation	30
Appendix I	Objectives, Scope, and Methodology	33
Appendix II	Requirements and Components of PIV-II	35
Appendix III	Selected NIST Guidance	37
Appendix IV	Comments from the Office of Management and Budget	40
Appendix V	GAO Contact and Staff Acknowledgments	45
Glossary		46
Tables		
	Table 1: The Three PIV Card Authentication Capabilities and Their Associated Assurance Levels	13

Table 2: Agencies' Progress in Implementing Background Checks and Basic Infrastructure and in Using the PIV Cards for Physical and Logical Access Control as of December 1, 2007	21
Table 3: Disparate Guidance for Physical Access Control	26

Figures

Figure 1: A Typical Smart Card	7
Figure 2: A PIV Card Showing Major Physical Features	12
Figure 3: Major Activities of the PIV System and Its Intended Day-to-Day Use	14
Figure 4: Timeline of HSPD-12-Related Activities	17

Abbreviations

CHUID	cardholder unique identifier
DHS	Department of Homeland Security
DOJ	Department of Justice
FIPS	Federal Information Processing Standards
GSA	General Services Administration
GSC-IS	Government Smart Card Interoperability Specification
HSPD-12	Homeland Security Presidential Directive 12
HUD	Department of Housing and Urban Development
ID	identification
MSO	Managed Service Office
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OMB	Office of Management and Budget
PIN	personal identification number
PIV	personal identity verification
PKI	public key infrastructure
USDA	U.S. Department of Agriculture

This is a work of the U.S. government and is not subject to copyright protection in the United States. This 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.



United States Government Accountability Office
Washington, DC 20548

February 29, 2008

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

The Honorable Edolphus Towns
Chairman
The Honorable Brian Bilbray
Ranking Member
Subcommittee on Government Management,
Organization, and Procurement
Committee on Oversight and Government Reform
House of Representatives

As you know, wide variations exist in the quality and security of the various forms of identification (ID) that federal agencies issue to their employees to use to access federal facilities and information systems. In an effort to increase the quality and security of ID and credentialing practices across the federal government, 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 ID for federal government employees and contractors who access government-controlled facilities and information systems. In addition, one of the primary goals of HSPD-12 is to enable interoperability across federal agencies.

In February 2005, the Department of Commerce's National Institute of Standards and Technology (NIST) issued Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification of Federal Employees and Contractors*. Known as FIPS 201, the standard is divided into two parts. The first part, personal identity verification (PIV)-I, sets out uniform requirements for identity proofing—verifying the identity of individuals applying for official agency credentials—and for issuing credentials, maintaining related information, and protecting the privacy of the applicants. The Office of Management and Budget (OMB), which is responsible for ensuring compliance with the standard, issued guidance

requiring agencies to implement these requirements, with the exception of the privacy requirements, by October 27, 2005. The second part, PIV-II, specifies the technical requirements for credentialing systems for federal employees and contractors on the basis of interoperable¹ smart cards.² OMB directed that by October 27, 2007, PIV credentials be issued to and used by all employees and contractors who have been with the agency for 15 years or less. It also directed that the remainder of the employees be issued cards and begin using their cards no later than October 27, 2008.

In February 2006, we reported on agencies' progress toward implementing the first part of the standard, PIV-I.³ This report responds to your request that we conduct a review of agencies' progress in implementing the second part of the standard, PIV-II. Specifically, our objectives were to determine the progress selected agencies have made in (1) implementing the capabilities of the PIV cards to enhance security and (2) achieving interoperability with other agencies.

To address these objectives, we selected eight agencies that have a range of experience in implementing smart card-based ID systems—the Departments of Agriculture (USDA), Commerce, the Interior, Homeland Security (DHS), Housing and Urban Development (HUD), and Labor; the Nuclear Regulatory Commission (NRC); and the National Aeronautics and Space Administration (NASA). To obtain information on the agencies' progress, we analyzed documentation such as agencies' high-level plans for HSPD-12 implementation, system architectures, cost estimates, and documentation of agencies' implementation activities. We also interviewed program officials from these agencies as well as General Services Administration (GSA), OMB, and NIST officials who have been involved in supporting implementation of HSPD-12 across the government. We also discussed implementation challenges with industry experts to obtain additional information and their perspectives. To obtain information on agencies' progress toward achieving cross-agency interoperability, we

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

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 information but cannot process or exchange data with automated information systems.

³GAO, *Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, [GAO-06-178](#) (Washington, D.C.: Feb. 1, 2006).

reviewed and analyzed documentation, such as existing interface specifications, and met with GSA officials and industry experts to discuss the steps they have taken to establish cross-agency interoperability.

We performed our work at Commerce, DHS, GSA, HUD, Interior, Labor, NASA, NIST, NRC, OMB, and USDA in the Washington, D.C., metropolitan area from June 2007 to February 2008. We conducted this 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. Also, we provide a glossary of terms at the end of this report.

Results in Brief

Much work has been accomplished to lay the foundations for implementation of HSPD-12, a major governmentwide undertaking. However, agencies have made limited progress in implementing and using PIV cards. The eight agencies we reviewed have generally completed background checks on most of their employees and contractors and established basic infrastructure, such as purchasing card readers. However, none of the agencies met OMB's goal of issuing PIV cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that have been issued, agencies generally have not been using the electronic authentication capabilities on the cards and have not developed implementation plans for those authentication mechanisms. Key products have not been available to support all of those capabilities. A key contributing factor for why agencies have made limited progress in adopting the use of PIV cards is that OMB, which is tasked with ensuring that federal agencies successfully implement HSPD-12, has emphasized the issuance of cards, rather than the full use of the cards' capabilities. Specifically, OMB has set milestones that focus narrowly on having agencies acquire and issue cards in the near term, regardless of when the electronic authentication capabilities of the cards could be used. Furthermore, agencies anticipate having to make substantial financial investments to implement HSPD-12, since PIV cards are considerably more expensive than traditional ID cards. For example, PIV cards and related services, offered by GSA, cost \$226 per card over the 5-year life of a card, whereas traditional ID credentialing systems with little or no electronic authentication capabilities cost significantly less. However, OMB does not

consider the implementation of HSPD-12 to be a major new investment. As a result, OMB has not directed agencies to prepare detailed plans to support their decisions regarding how, when, and the extent to which they will implement the various electronic authentication capabilities. Furthermore, without implementing the cards' electronic authentication capabilities, agencies will continue to purchase costly PIV cards and use them in the same way as the much cheaper, traditional ID cards they are replacing. Until OMB revises its approach to focus on the full use of card capabilities, HSPD-12's objectives of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

While steps have been taken to enable future interoperability, progress has been limited in implementing such capabilities in current systems, partly because key procedures and specifications have not yet been developed to enable electronic cross-agency authentication of cardholders. According to GSA officials, they have taken the initial steps to develop guidance to help enable the exchange of identity information across agencies, and they plan to complete and issue it by September 2008.

We are making recommendations to OMB to revise its approach to overseeing the implementation of HSPD-12, including establishing realistic milestones for implementation of electronic authentication capabilities and treating HSPD-12 implementation as a major new investment by requiring that each agency develop detailed plans that support its decisions regarding how, when, and the extent to which it will implement the electronic authentication capabilities of the cards.

We received written comments on a draft of this report from the Administrator of the Office of E-Government and Information Technology of OMB. The letter is reprinted in appendix IV. We also received written technical comments from the director of the DHS liaison office for GAO and the Office of the Inspector General, the Associate Deputy Secretary of the Interior, the Administrator of GSA, a Program Specialist from NASA, and the Acting Chief Information Officer for Commerce. The Deputy Assistant Secretary for Administration and Management from Labor provided technical oral comments, and a senior policy analyst from OMB provided technical comments via e-mail. We have incorporated these comments, as appropriate. In addition, a GAO liaison from NRC indicated via e-mail, and the Assistant Secretary for Administration of HUD stated in writing, that their respective agency officials had reviewed the draft report and did not have any comments. Officials from USDA did not respond to our request for comments.

OMB provided comments on our recommendations but did not specifically agree or disagree with any of them. Furthermore, in subsequent discussions, OMB staff declined to agree or disagree with our recommendations, indicating that they did not want to characterize their comments in those terms.

Regarding our recommendation that OMB establish realistic milestones for full implementation of the infrastructure needed to best use the electronic authentication capabilities of PIV cards, the agency stated that its guidance requires agencies to provide milestones for when they intend to leverage the capabilities of PIV credentials. However, to ensure consistent governmentwide implementation of HSPD-12, it is important for OMB to establish such milestones across agencies, rather than to allow individual agencies to choose their own milestones. By not setting time frames for agencies to implement this infrastructure, OMB has left it uncertain when these capabilities, which are critical to the success of HSPD-12, should be implemented across the government.

Regarding our recommendation that it require each agency to develop a risk-based, detailed plan for implementing electronic capabilities, OMB stated that previous guidance required agencies to provide milestones for when they plan to fully leverage the capabilities of PIV credentials for physical and logical access control. However, agencies were required to provide only the dates they plan to complete major activities, such as becoming fully compliant with HSPD-12 and having a plan for phasing in physical and logical access control. OMB did not require agencies to develop detailed, risk-based plans.

Regarding our recommendation that OMB require agencies to align the acquisition of PIV cards with plans for implementing the cards' electronic authentication capabilities, OMB stated that HSPD-12 aligns with other information security programs. While OMB's statement is correct, it is important that agencies time the acquisition of PIV cards to coincide with the implementation of the technical infrastructure necessary for enabling electronic authentication techniques.

Regarding our recommendation that OMB ensure that guidance is developed that maps existing physical security guidance to FIPS 201 guidance, the agency stated that NIST is in the process of developing additional guidance to clarify the relationship between facility security levels and PIV authentication levels. Until complete guidance is available, agencies will likely continue either to delay in making decisions on their implementations or to make decisions that may need to be modified later.

Background

Historically, federal employees have been issued a wide variety of ID cards that are used to access federal buildings and other facilities. In many cases, security personnel allow access on the basis of visual inspection of these cards. However, many of these cards can be easily forged and have other limitations in their ability to effectively authenticate individuals seeking access to federal facilities.

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/or exit of users from 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.

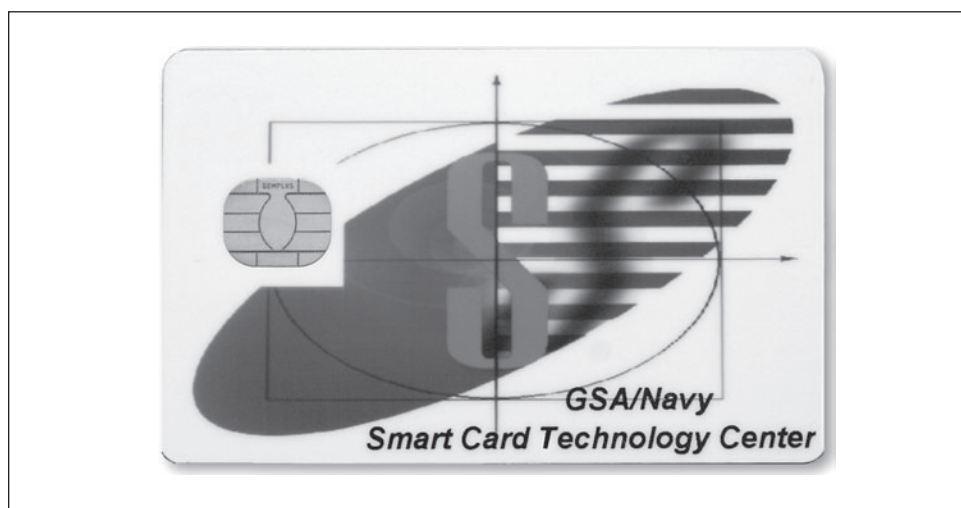
Access control techniques vary in the extent to which they can provide assurance that only authorized individuals and systems have been granted access. Some techniques can be easily subverted, while others are more difficult to circumvent. Generally, techniques that provide higher levels of assurance are more expensive, more difficult to implement, and cause greater inconvenience to users than less sophisticated techniques. 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.⁴ 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. Figure 1 shows an example of a typical smart card.

Figure 1: A Typical Smart Card



Source: GSA.

Smart cards can also be used to significantly enhance the security of an agency's computer systems by tightening controls over user access. A user wishing to log on to a computer system or network with controlled access must "prove" his or her identity to the system—a process called authentication. Many systems authenticate users by requiring them to

⁴The 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.

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 would not only need to guess a user's password but would also need to possess that same user's smart card.

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 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.⁵

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.⁶ 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

⁵For more information about biometrics, see GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 15, 2002).

⁶For 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).

to have two different digital “keys” to gain access: a public key and a private key. Both public and private keys may be generated on a smart card or on a user’s computer. 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 manage electronic “certificates” that link an individual or entity to a given public key. These digital certificates are then used to verify digital signatures and facilitate data encryption. The digital certificates are created by a trusted third party called a certification authority, which is also responsible for providing 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 online status information to ensure that it has not been revoked or suspended.

Implementing a functioning PKI across government agencies involves much more than just establishing the basic hardware and software infrastructure at individual agencies. For example, for PKI certificates to work across the government, a vast network of interoperable online directories would need to be in place so that each user’s identity could be looked up and his or her digital certificate verified before any transaction takes place. Software applications would likely need to consult a number of disparate directories to validate an incoming user’s digital certificate. Significant costs are involved in developing, fielding, and maintaining a production PKI to meet these requirements. Systems must be set up to positively identify users and manage the exchange and verification of certificates. In addition, existing software applications, electronic directories, and other legacy systems must be modified so that they can interact with the PKI. As a result, the total costs associated with building a PKI and enabling applications to use it can be significant.

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 contractors to enable interoperability across the federal government by February 27, 2005. The directive defined secure and reliable ID as meeting four control objectives. Specifically, the identification credentials must be

- based on sound criteria for verifying an individual employee’s or contractor’s identity;

-
- strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
 - able to be rapidly authenticated electronically; and
 - issued only by providers whose reliability has been established by an official accreditation process.

HSPD-12 stipulates that the standard must include criteria that are graduated from “least secure” to “most secure” to ensure flexibility in selecting the appropriate level of security for each application. In addition, the directive directs agencies to implement, to the maximum extent practicable, the standard for IDs issued to federal employees and contractors in order to gain physical access to controlled facilities and logical access to controlled information systems by October 27, 2005.⁷

FIPS 201: Personal Identity Verification of Federal Employees and Contractors

In response to HSPD-12, 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 contractors for gaining physical access to federal facilities and logical access to information systems and software applications. Smart cards are a primary component of the envisioned PIV system.

The FIPS 201 standard is composed of two parts. 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 interoperable smart card-based PIV systems.

Personal Identity Verification I

To verify individuals’ identities, 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,

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

⁸NIST’s SP 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, describes a set of attributes that should be exhibited by a PIV card issuer in order to be accredited. The guidelines should be used by each agency for assessing the reliability of any potential contractor for PIV card-issuing services.

such as completing a background investigation of the applicant,⁹ conducting and adjudicating a fingerprint check prior to credential issuance, and requiring applicants to provide two original forms of identity source documents from an OMB-approved list of documents.

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

As we have previously mentioned, the second part of the FIPS 201 standard, PIV-II, provides technical specifications for interoperable smart card-based PIV systems. The components and processes in a PIV system, as well as the identity authentication information included on PIV cards, are intended to provide for consistent authentication methods across federal agencies. The PIV-II cards (see example in fig. 2) 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.

⁹Prior to HSPD-12, agencies were generally conducting some form of a background check on their employees; however, the quality and consistency of the background checks varied among agencies. FIPS 201 established a minimum standard that all agencies must meet for conducting background checks on employees and contractors.

Figure 2: A PIV Card Showing Major Physical Features



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

The PIV cards contain a range of features—including photographs, cardholder unique identifiers (CHUID), fingerprints, and PKI certificates—to enable enhanced identity authentication at different assurance levels. To use these enhanced capabilities, specific infrastructure needs to be in place. This infrastructure may include biometric (fingerprint) readers, personal ID number (PIN) input devices, and connections to information systems that can process PKI digital certificates and 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.

FIPS 201 includes specifications for three types of electronic authentication that provide varying levels of security assurance. OMB guidance and FIPS 201 direct agencies to use risk-based methods to decide which type of authentication is appropriate in a given circumstance. The

three authentication methods for PIV cards specified under FIPS 201 and their associated assurance levels are described in table 1.

Table 1: The Three PIV Card Authentication Capabilities and Their Associated Assurance Levels

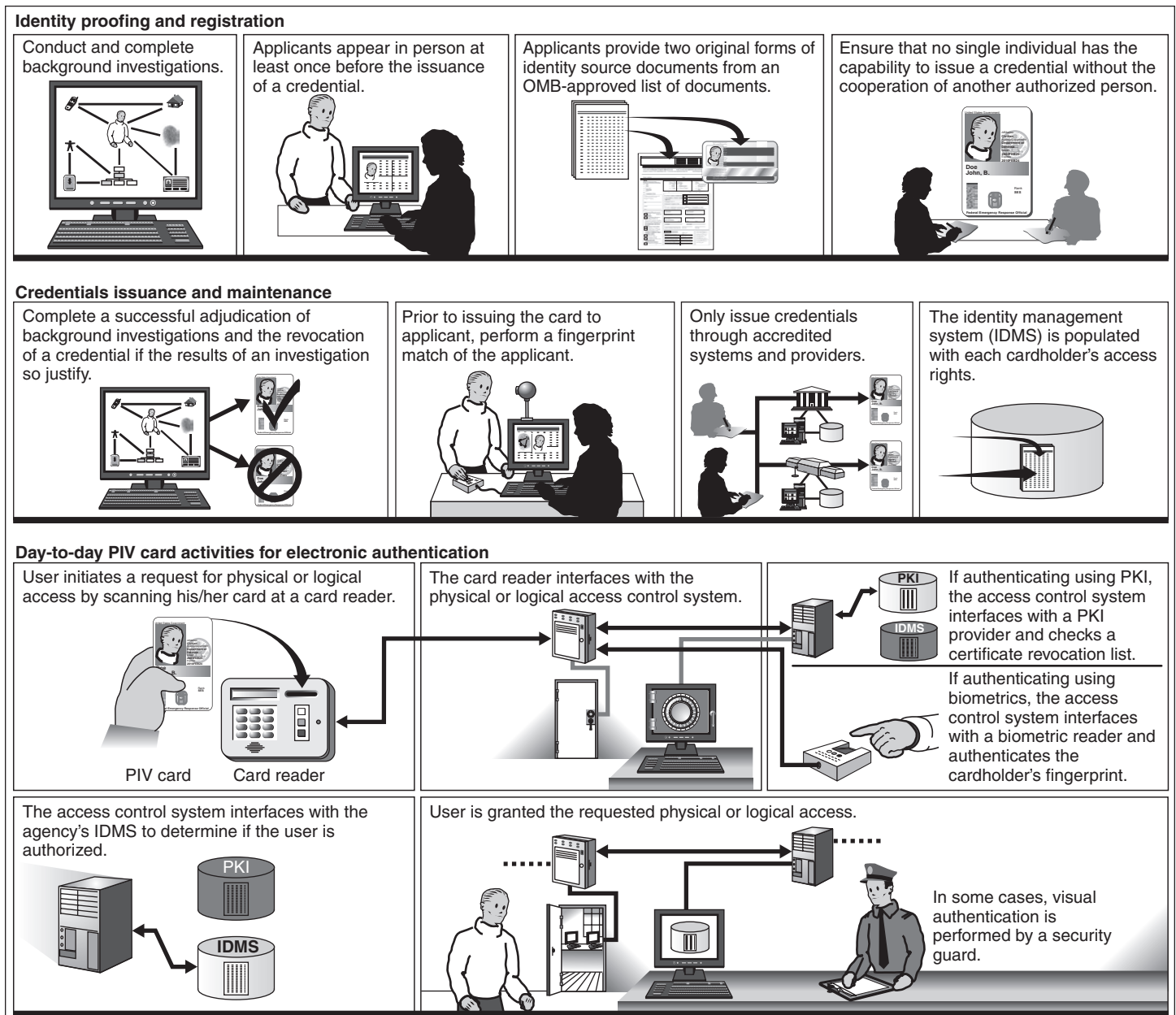
	CHUID authentication or visual authentication (some confidence)	Biometric authentication only (high confidence)	PKI authentication and/or biometric authentication with visual authentication (very high confidence)
Description of authentication capability	The CHUID is a number comprising several pieces 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 inspection consists of a guard visually comparing the photograph on the card with the cardholder.	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 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.
Description of assurance level	Use of the CHUID provides limited assurance, since it is not encrypted and is able to authenticate only the card, not the cardholder. According to NIST officials, use of only the CHUID may be appropriate in very limited circumstances. For example, once a cardholder has been authenticated using both the CHUID and visual inspection to get into a federal facility, it may be appropriate to use just the CHUID for accessing relatively low security/criticality areas within the facility. Similarly, according to NIST officials, exclusive use of visual inspection may also be appropriate in limited circumstances, such as at a federal office that has very few employees.	Biometric authentication without the presence of a security guard or attendant at the access point offers a high level of assurance of the cardholders' identity.	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.

Source: GAO analysis of FIPS 201 and related guidance.

In addition to the three 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.

Figure 3 illustrates the major activities of the PIV system and its intended day-to-day use.

Figure 3: Major Activities of the PIV System and Its Intended Day-to-Day Use



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

Additional NIST, GSA, and OMB Guidance

NIST has 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, which are intended to ensure that products and services meet FIPS 201 requirements. The GSA tests include products that have successfully passed NIST's conformance tests as well as other products that are directed by FIPS 201 but 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 listed on its list of products that are approved for agencies to acquire.

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

- October 27, 2005—For all new employees and contractors, adhere to the identity proofing, registration, card issuance, and maintenance requirements of the first part (PIV-I) of the standard.
- October 27, 2006—Begin issuing cards that comply with the second part (PIV-II) of the standard and implementing the privacy requirements.
- October 27, 2007—Verify and/or complete background investigations for all current employees and contractors who have been with the agency for

15 years or less. Issue PIV cards to these employees and contractors and require that they begin using their cards by this date.

- October 27, 2008—Complete background investigations for all individuals who have been federal agency employees for more than 15 years. Issue cards to these employees and require them to begin using their cards by this date.¹⁰

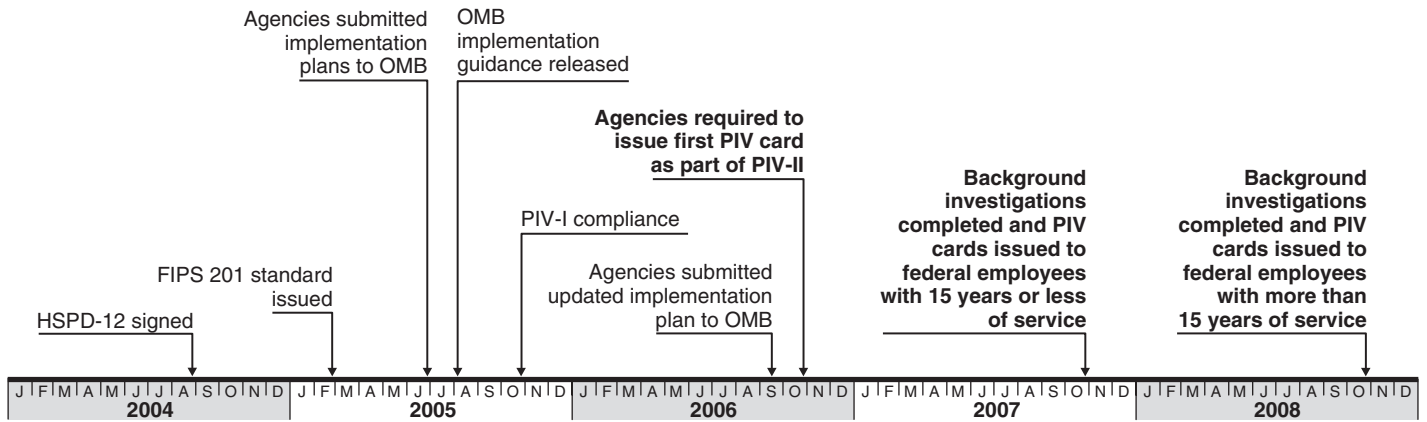
In addition, OMB directed that each agency provide certain information on its plans for implementing HSPD-12, including the number of individuals requiring background checks and the dates by which the agency plans to be compliant with PIV-I and PIV-II requirements. Agencies were not directed to provide information on the cost of their implementations, but they were directed to submit this information to OMB by June 29, 2005. Subsequently, agencies were directed to submit updated planning information to OMB by September 8, 2006. Finally, after the October 27, 2007, milestone had passed, OMB requested that agencies provide it with an updated plan.

Other related guidance that OMB has 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 memorandum to agencies on safeguarding against and responding to the breach of personally identifiable information, and updated instructions to agencies on publicly reporting their HSPD-12 implementation status.

Figure 4 shows a timeline that illustrates when HSPD-12 and additional guidance was issued as well as the major deadlines for implementing HSPD-12.

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

Figure 4: Timeline of HSPD-12-Related Activities



Source: GAO analysis of FIPS 201 guidance.

GSA, in collaboration with the Federal Identity Credentialing Committee,¹¹ the Federal Public Key Infrastructure Policy Authority,¹² OMB, and the Smart Card Interagency Advisory Board¹³—which GSA established to address government smart card issues and standards—developed the *Federal Identity Management Handbook*. This handbook was intended to be a guide for agencies in implementing HSPD-12 and FIPS 201 and includes guidance on specific courses of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies. It is to be periodically updated; the most current version of the handbook was released in December 2005.

On June 30, 2006, GSA and OMB issued a memorandum to agency officials that specified standardized procedures for acquiring FIPS 201-compliant commercial products that have passed NIST's and GSA's testing. According to the GSA guidance, agencies are directed to use these

¹¹The Federal Identity Credentialing Committee is composed of representatives from federal agencies and departments and is intended to assist agencies in implementing governmentwide credentialing capabilities.

¹²The Federal Public Key Infrastructure Policy Authority is an interagency body that is under the Chief Information Officers Council. It enforces digital certificate standards for trusted identity authentication across the federal government.

¹³The Smart Card Interagency Advisory Board is composed of representatives from federal agencies and is intended to share information with federal agency and private sector representatives regarding HSPD-12 implementation activities.

standardized acquisition procedures when implementing their FIPS 201-compliant systems.

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 October 2007, GSA had 67 agency customers with more than 700,000 government employees and contractors to whom cards would be issued through shared service providers. In addition, as of December 31, 2007, the Managed Service Office (MSO) had installed over 50 enrollment stations with 15 agencies actively enrolling employees and issuing PIV cards. While there are several services offered by the MSO, it is not intended to provide support for all aspects of HSPD-12 implementation. For example, the MSO does not provide services to help agencies integrate their physical and logical access control systems with their PIV systems.

In 2006, GSA's Office of Governmentwide Policy established the interagency HSPD-12 Architecture Working Group, which is intended to develop interface specifications for HSPD-12 system interoperability across the federal government. As of July 2007, the group had issued 10 interface specification documents, including a specification for exchanging data between an agency and a shared service provider.

Previously Reported FIPS 201 Implementation Challenges

In February 2006, we reported that agencies faced several challenges in implementing FIPS 201, including constrained testing time frames and funding uncertainties as well as incomplete implementation guidance.¹⁴ We recommended that OMB monitor agencies' implementation process and completion of key activities. In response to this recommendation, beginning on March 1, 2007, OMB directed agencies to post to their public Web sites quarterly reports on the number of PIV cards they had issued to their employees, contractors, and other individuals. In addition, in August 2006, OMB directed each agency to submit an updated implementation plan.

¹⁴[GAO-06-178](#).

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

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

Agencies have made limited progress in implementing and using PIV cards. While the eight agencies we reviewed have generally taken steps to complete background checks on most of their employees and contractors and establish basic infrastructure, such as purchasing card readers, none of the agencies met OMB's goal of issuing PIV cards by October 27, 2007, to all employees and contractor personnel who had been with the agency for 15 years or less. In addition, for the limited number of cards that have been issued, agencies generally have not been using the electronic authentication capabilities on the cards and have not developed implementation plans for those capabilities. Key products are not available to support all of those capabilities.

A key contributing factor for why agencies have made limited progress in adopting the use of PIV cards is that OMB, which is tasked with ensuring that federal agencies successfully implement HSPD-12, has focused agencies' attention on card issuance, rather than on full use of the cards' capabilities. Specifically, OMB set milestones that focused narrowly on having agencies acquire and issue cards in the near term, regardless of when the electronic authentication capabilities of the cards could be used. Furthermore, although agencies anticipate having to make substantial financial investments to implement HSPD-12, OMB has not considered this to be a major new investment and has not directed agencies to prepare detailed plans to support their decisions regarding how, when, and the extent to which they plan to implement the cards' electronic authentication capabilities.

Without implementing these capabilities, agencies will continue to purchase costly PIV cards to be used in the same way as the much cheaper, traditional ID cards they are replacing. More significantly, until OMB revises its approach to focus on the full use of card capabilities, HSPD-12's objective of increasing the quality and security of ID and credentialing practices across the federal government may not be fully achieved.

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

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

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

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

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

Table 2 provides details about the progress each of the eight agencies had made as of December 1, 2007.

Table 2: Agencies' Progress in Implementing Background Checks and Basic Infrastructure and in Using the PIV Cards for Physical and Logical Access Control as of December 1, 2007

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

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

Source: GAO analysis of documentation provided by agency officials.

^aThese data are as reported by the agencies.

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

^cAccording to DHS officials, the public release of the total number of employees requiring and carrying DHS PIV cards could pose a security risk.

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

^eThis infrastructure is being supplied by GSA's MSO.

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

Products to Use Certain
Electronic Authentication
Capabilities Have Not Been
Available

Three of the eight agencies we reviewed—HUD, NASA, and USDA—indicated that, while they were not currently using the enhanced authentication capabilities, they were in the process of testing products, such as biometric readers and readers that can access and authenticate PKI certificates, to determine whether they could be integrated into their agencies' existing access control systems.

A challenge to full use of the enhanced authentication capabilities of PIV cards is that key products have not yet been commercially available. As a result, agencies have been constrained in their ability to build systems that use key authentication capabilities.

Currently available products are only partially able to implement electronic authentication based on the CHUID that is included on all PIV cards. The CHUID is a special type of serial number that incorporates an electronic signature and is used to electronically validate that the information contained in the CHUID, such as the card expiration date, has not been altered. However, existing physical access control systems are unable to receive and process a full CHUID, which is up to 27,016 bits long. Most legacy control panels for physical access control systems were built to process only a 26-bit identification number, and even the newest control panels are only able to process 256 bits, at best. Consequently, agencies that have implemented CHUID-based authentication have had to implement systems that truncate the CHUID so that only a subset of information—without the electronic signature—is transmitted to the control panel for authentication. Use of the truncated CHUID does not provide the same level of assurance as processing the full CHUID, because the electronic signature information is not included. According to industry representatives, it could take at least 5 to 7 years before a physical access control system could be commercially available that is capable of reading the full CHUID. Depending on the risk level of a system or facility, using the truncated CHUID authentication approach could have important security implications.

Another product not yet on the market is a PIV card reader that can access and validate the PKI certificate on a PIV card. According to industry representatives, it will be expensive to develop such readers, and many industry suppliers are not involved because they do not anticipate that they will be able to market these readers to organizations outside of the federal government. The industry representatives indicated that a few companies that have a federal government focus are developing products for this application, and they anticipate that products will become available later in 2008.

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

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

OMB's Implementation Milestones Have Been Narrowly Focused

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

The PIV card and the services involved in issuing and maintaining the data on the card, such as the PKI certificates, are costly. For example, PIV cards and related services offered by GSA through its shared service offering cost \$82 per card for the first year and \$36 per card for each of the remaining 4 years of the card's life. In contrast, traditional ID cards with limited or no electronic authentication capabilities can cost less than \$1 each, and have no annual maintenance costs. Therefore, agencies that do not implement electronic authentication techniques are spending a considerable amount per card for capabilities that they are not able to use. An agency such as Interior, for example, which plans to issue cards to approximately 90,000 individuals, could potentially spend approximately \$20 million on PIV cards without realizing the benefits of those cards until it implements their electronic authentication capabilities. A more economical approach would be to establish detailed plans for implementing the technical infrastructure necessary to use the electronic authentication capabilities on the cards and time the acquisition of PIV

OMB Has Not Considered
HSPD-12 Implementation to Be
a Major New Investment

cards to coincide with the implementation of this infrastructure. However, this approach has not been encouraged by OMB, which instead has been measuring agencies on how many cards they issue.

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

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

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

While OMB has not directed agencies to develop business cases for HSPD-12 implementation efforts, PIV card systems are likely to represent significant new investments at several agencies. For example, agencies such as Commerce, HUD, and Labor had not implemented PKI technology prior to HSPD-12, but they are now directed to do so. In addition, such agencies’ previous ID cards were used for limited purposes and were not used for logical access. These agencies had no prior need to acquire or maintain card readers for logical access control or to establish connectivity with their ID management systems for logical access control and, consequently, had previously allocated very little money for the operations and maintenance of these systems. Specifically, HUD’s annual operations and maintenance costs for its pre-HSPD-12 legacy system totaled approximately \$127,000, while the agency’s estimated cost for

HSPD-12 implementation in fiscal year 2008 is approximately \$1.6 million—about 13 times more expensive. According to Labor officials, operations and maintenance costs for its pre-HSPD-12 legacy system totaled approximately \$169,000, and Labor’s fiscal year 2009 budget request for HSPD-12 implementation is approximately \$3 million—17 times more expensive.

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

While the technical requirements of complying with HSPD-12 dictate that a major new investment be made, generally, agencies have not been directed by OMB to take the necessary steps to thoroughly plan for these investments. For example, six of the eight agencies we reviewed had not developed detailed plans regarding their use of PIV cards for physical and logical access controls. In addition, seven of the eight agencies had not prepared cost-benefit analyses that weighed the costs and benefits of implementing different authentication capabilities.

Without treating the implementation of HSPD-12 as a major new investment by requiring agencies to develop detailed plans based on risk-based assessments of agencies’ physical and logical access control needs that support the extent to which electronic authentication capabilities are to be implemented, OMB will continue to limit its ability to ensure that agencies properly plan and implement HSPD-12. As a result, HSPD-12 implementation may not achieve enhanced access control, and agencies may make considerable expenditures to acquire capabilities that they cannot use.

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

Another factor contributing to agencies’ limited progress is that OMB has not provided guidance to agencies regarding how to determine which electronic authentication capabilities to implement for physical and logical access controls. While the FIPS 201 standard describes three different assurance levels for physical access (some, high, and very high confidence) and associates PIV authentication capabilities with each level, it is difficult for agencies to link these assurance levels with existing building security assurance standards that are used to determine access controls for facilities. The Department of Justice (DOJ) has developed

standards for assigning security levels to federal buildings, ranging from level I (typically, a leased space with 10 or fewer employees, such as a military recruiting office) to level V (typically, a building such as the Pentagon or Central Intelligence Agency headquarters that has a large number of employees and a critical national security mission). While there are also other guidelines that agencies could use to conduct assessments of their buildings, several of the agencies we reviewed use the DOJ guidance to conduct risk assessments of their facilities. Table 3 compares these disparate sets of guidance for physical access control.

Table 3: Disparate Guidance for Physical Access Control

NIST's FIPS 201 standards		DOJ standards	
PIV confidence level	PIV authentication capability	DOJ security level	Standards
Some confidence	CHUID or visual	Level I	Ten or fewer federal employees, very small office space (2,500 or less square feet), and low volume of public contact
High confidence	Biometric check	Level II	From 11 to 150 federal employees, small office space (2,500 to 80,000 square feet), and moderate volume of public contact
Very high confidence	PKI and/or biometric check, and visual check	Level III	From 151 to 450 federal employees, medium-size office space (80,000 to 150,000 square feet), and moderate-to-high volume of public contact
		Level IV	Over 450 federal employees, large office space (more than 150,000 square feet), and high volume of public contact
		Level V	Similar characteristics of level IV, and contains mission functions critical to national security (e.g., the Pentagon)

Source: GAO analysis of NIST and DOJ guidance.

Officials from several of the agencies we reviewed indicated that they were not using the FIPS 201 guidance to determine which PIV authentication capabilities to use for physical access because they did not find the guidance to be complete. Specifically, they were unable to determine which authentication capabilities should be used for the different security levels. The incomplete guidance has contributed to

several agencies—including Commerce, DHS, and NRC—not reaching decisions on what authentication capabilities they were going to implement.

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

Agencies also lack guidance regarding when to use the enhanced authentication capabilities for logical access control. Similar to physical access control, FIPS 201 describes graduated assurance levels for logical access (some, high, and very high confidence) and associates PIV authentication capabilities with each level. However, as we have previously reported, neither FIPS 201 nor supplemental OMB guidance provides sufficient specificity regarding when and how to apply the standard to information systems.¹⁵ For example, such guidance does not inform agencies how to consider the risk and level of confidence needed when different types of individuals require access to government systems, such as a researcher uploading data through a secure Web site or a contractor accessing government systems from an off-site location.

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

¹⁵GAO-06-178.

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

One of the primary goals of HSPD-12 is to enable interoperability across federal agencies. As we have previously reported, prior to HSPD-12, there were wide variations in the quality and security of ID cards used to gain access to federal facilities.¹⁶ To overcome this limitation, HSPD-12 directed ID cards to have standard features and means for authentication to enable interoperability among agencies.

While steps have been taken to enable future interoperability, progress has been limited in implementing such capabilities in current systems, partly because key procedures and specifications have not yet been developed. As we have previously stated, NIST has established conformance testing for the PIV card and interface, and GSA has established testing for other PIV products and services to help enable interoperability. In addition, the capability currently exists for determining the validity and status of a cardholder from another agency via PKI. However, procedures and specifications to enable cross-agency interoperability using the CHUID—which is expected to be more widely used than PKI—have not been established. While PIV cards and FIPS 201-compliant readers may technically be able to read the information encoded on any PIV card—including cards from multiple agencies—this functionality is not adequate to allow one agency to accept another agency’s PIV card, because there is no common interagency framework in place for agencies to electronically exchange status information on PIV credentials. For example, the agency that issued a PIV card could revoke the cardholder’s authorization to access facilities or systems if the card is lost or if there has been a change in the cardholder’s employment status. The agency attempting to process the card would not be able to access this information because a common framework to electronically exchange status information does not exist. The interfaces and protocols that are needed for querying the status of cardholders have not yet been developed.

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

¹⁶ [GAO-06-178](#).

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

Conclusions

While HSPD-12's objective was to eliminate wide variations in the quality and security of forms of ID used to gain access to federal facilities, agencies have made limited progress in implementing and using PIV cards in ways that would achieve this objective. Although they did not meet OMB's October 2007 milestone for card issuance, agencies have nevertheless focused on issuing cards to employees and contractor personnel without developing plans for using the electronic authentication capabilities of the cards. These agency actions have been driven by OMB's guidance, which has emphasized the issuance of cards, rather than the full use of the cards' capabilities. While setting ambitious goals and objectives can help ensure that an initiative is given priority, OMB's milestones did not provide a focus on implementing the electronic capabilities available through the PIV cards. Furthermore, agencies' milestones for issuing the cards did not coincide with the implementation of the technical infrastructure. Despite the cost of the cards and associated infrastructure, OMB has not treated the implementation of HSPD-12 as a major new investment and has not ensured that agencies have guidance to ensure consistent and appropriate implementation of electronic authentication capabilities across agencies for physical and logical access. Until these issues are addressed, agencies will likely continue to acquire and issue costly PIV cards and not be able to use their advanced capabilities.

In addition, much work remains before agencies can take advantage of the potential for interoperability under HSPD-12. GSA officials have taken initial steps to develop guidance to help enable the exchange of identity information across agencies, and they plan to complete and issue guidance by September 2008. Such guidance should help enable agencies to establish cross-agency interoperability—a primary goal of HSPD-12.

Recommendations for Executive Action

We recommend that the Director, Office of Management and Budget, revise the agency's approach to overseeing implementation of HSPD-12 by taking the following four actions:

- Establish realistic milestones for full implementation of the infrastructure needed to best use the electronic authentication capabilities of PIV cards in agencies.
- Treat the HSPD-12 implementation as an investment by requiring that each agency develop a detailed plan, based on a risk-based assessment of the agency's physical and logical access control needs, that supports the extent to which electronic authentication capabilities are to be implemented.
- Require agencies to align the acquisition of PIV cards with plans for implementing their technical infrastructure to best use the cards' electronic authentication capabilities.
- Ensure that guidance is developed that maps existing physical security guidance to FIPS 201 guidance.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from OMB's Administrator of the Office of E-Government and Information Technology. The letter is reprinted in appendix IV. In addition to OMB's letter, an OMB senior policy analyst also provided technical comments via e-mail, which we have incorporated as appropriate. We also received written technical comments from the director of the DHS liaison office for GAO and the Office of the Inspector General, the Associate Deputy Secretary of the Interior, the Administrator of GSA, a program specialist at NASA, and the Acting Chief Information Officer for Commerce. The Deputy Assistant Secretary for Administration and Management from Labor provided oral technical comments. We have incorporated these comments as appropriate. In addition, a GAO liaison from NRC indicated via e-mail, and the Assistant Secretary for Administration of HUD stated in writing that their respective agency officials had reviewed the draft report and did not have any comments. USDA officials did not respond to our request for comments.

OMB provided comments on our recommendations but did not specifically agree or disagree with any of them. Also, in subsequent discussions, OMB staff declined to agree or disagree with our recommendations, indicating that they did not want to characterize their comments in those terms.

Regarding our recommendation that OMB establish realistic milestones for full implementation of the infrastructure needed to best use the electronic authentication capabilities of PIV cards, the agency stated that it agrees that it is important to set milestones for implementing the necessary infrastructure, and that its guidance requires agencies to provide milestones for when they intend to leverage the capabilities of PIV credentials. However, to ensure consistent governmentwide implementation of HSPD-12, it is important for OMB to establish such milestones across agencies, rather than to allow individual agencies to choose their own milestones. By not setting time frames for agencies to implement this infrastructure, OMB has left it uncertain when these capabilities, which are critical to the success of HSPD-12, should be implemented across the government.

Regarding our recommendation that OMB require each agency to develop a risk-based, detailed plan for implementing electronic capabilities, the agency stated that previous guidance required agencies to develop implementation plans and provide milestones for when they plan to fully leverage the capabilities of PIV credentials for physical and logical access controls. However, the implementation plans that OMB refers to are based on a template that requires agencies to provide only the dates they plan to complete major activities, such as becoming fully compliant with HSPD-12 and having a plan for phasing in physical and logical access controls. This template does not require that agencies develop detailed, risk-based plans, which would include an assessment of the cost of implementing advanced authentication capabilities and the rationale for specific implementation approaches. Without such detailed plans, agencies may not properly and consistently ensure that their HSPD-12 implementations make the best use of the cards' electronic capabilities or ensure that they are properly addressing high-risk areas.

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

Regarding our recommendation that OMB ensure guidance is developed that maps existing physical security guidance to FIPS 201 guidance, the

agency stated that NIST is in the process of developing additional guidance to clarify the relationship between facility security levels and PIV authentication levels. Until such guidance is available, agencies will likely continue either to delay in making decisions on their implementations or to make decisions that may need to be modified later.

OMB also provided additional comments, which we address in appendix IV.

Unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to interested congressional committees; the Secretaries of Homeland Security, Labor, Agriculture, Commerce, the Interior, and HUD; the Director of OMB; the Executive Director for Operations at NRC; and the Administrators of NASA and GSA. We will also make copies available to others upon request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staffs have any questions on the matters discussed in this report, please contact me at (202) 512-6240 or by e-mail at koontzl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix V.



Linda D. Koontz
Director, Information Management Issues

Appendix I: Objectives, Scope, and Methodology

Our objectives were to determine the progress that selected agencies have made in (1) implementing the capabilities of the personal identity verification (PIV) cards to enhance security and (2) achieving interoperability with other agencies. We reviewed Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standards (FIPS) 201, related Department of Commerce's National Institute of Standards and Technology (NIST) special publications, Office of Management and Budget (OMB) guidance, General Services Administration (GSA) guidance, and HSPD-12-related industry guidance. Using the results from the federal computer security report cards¹—which include an assessment of physical security—in conjunction with the results in GAO's most recent reports on federal agencies' progress in adopting smart card technology² and implementation of HSPD-12,³ on a nonprobability basis, we identified agencies that were in different stages of implementing smart card programs and were using different strategies for implementing HSPD-12. For example, we included agencies with no prior experience in implementing smart card systems as well as agencies with years of experience in implementing smart card systems. We also included agencies that were using GSA's shared services offering as well as agencies that were not. The agencies we selected were 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).⁴

To determine the progress selected agencies had made in implementing the capabilities of the HSPD-12-compliant cards, we analyzed documentation such as agencies' high-level plans for HSPD-12 implementation, system architectures, cost estimates, and documentation

¹The federal computer security report cards are prepared annually by the House Committee on Oversight and Government Reform, based on agencies' information security reports directed by the Federal Information Security Management Act of 2002.

²GAO, *Electronic Government: Progress in Promoting Adoption of Smart Card Technology*, [GAO-03-144](#) (Washington, D.C.: Jan. 3, 2003); and *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology*, [GAO-04-948](#) (Washington, D.C.: Sept. 8, 2004).

³GAO, *Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard*, [GAO-06-178](#) (Washington, D.C.: Feb. 1, 2006).

⁴We did not include the Department of Defense in this review because the department is taking an alternative approach to implementing HSPD-12 and, therefore, is not typical of federal agencies' experiences.

of agencies' implementation activities. We also interviewed officials from the selected agencies to obtain additional information on the actions their agencies took to implement PIV cards and the associated infrastructure. In addition, we compared the functionalities of the PIV card that each agency had implemented with the key functionalities that an agency could implement as set forth in FIPS 201.

We also interviewed GSA, NIST, and OMB officials to obtain additional information on guidance and agencies' efforts. We used the information provided by agency officials to identify the factors contributing to agencies' limited progress. We also presented the issues we identified to industry groups and obtained their feedback and additional information on the issues.

To determine agencies' progress toward achieving cross-agency interoperability, we reviewed and analyzed documentation from the Architecture Working Group, such as existing interface specifications. We obtained and analyzed briefings with status updates on plans to enable cross-agency authentication. We also met with GSA officials and industry experts to discuss the steps that have been taken to establish cross-agency interoperability. We used this information to identify what steps have been taken and what steps remain to establish cross-agency interoperability.

We performed our work at Commerce, DHS, GSA, HUD, Interior, Labor, NASA, NIST, NRC, OMB, and USDA in the Washington, D.C., metropolitan area from June 2007 to February 2008. We conducted this 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.

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 contractors 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.
- 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.
- Physical access control system—permits or denies a user access to a building or room. This system may employ 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 a PIV card and its authorizations by consulting an electronic database to determine whether the digital certificates contained on the card have been revoked.

Appendix III: Selected NIST Guidance

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

NIST SP 800-73-1, Interfaces for Personal Identity Verification, April 2006

SP 800-73-1 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 special publication aims to promote interoperability among PIV systems across the federal government by specifying detailed requirements intended to constrain vendors' interpretation of FIPS 201.¹ SP 800-73-1 also outlines two distinct approaches that agencies may take to become FIPS 201-compliant and specifies a set of requirements for each approach: one set for transitional card interfaces that are based on the Government Smart Card Interoperability Specification (GSC-IS), version 2.1, and another set for end-point card interfaces that are more fully compliant with the FIPS 201 PIV-II card specification. Federal agencies that have implemented smart card systems that are based on the GSC-IS can elect to adopt the transitional specification as an intermediate step before moving to the end-point specification. However, agencies with no existing implementation are directed to implement PIV systems that meet the end-point specification.

SP 800-73-1 includes requirements for both the transitional and end-point specifications and is divided into the following three parts:

- Part 1 specifies the requirements for a PIV data model that is designed to support dual interface (contact and contactless) cards. The mandatory data elements outlined in the data model are common to both the transitional and end-point interfaces and include strategic guidance for agencies that are planning to take the path of moving from the transitional interfaces to the end-point interfaces.
- Part 2 describes the transitional interface specifications and is for use by agencies with existing GSC-IS-based smart card systems.
- Part 3 specifies the requirements for the end-point PIV card and associated software applications.

¹“Interoperability” is defined as the use of PIV identity credentials, so that client-application programs, compliant card applications, and compliant integrated circuit cards can be used interchangeably by all information processing systems across the federal government.

NIST SP 800-85A, PIV Card Application and Middleware Interface Test Guidelines, April 2006

SP 800-85A outlines a suite of tests to validate a software developer's PIV middleware² and card applications to determine whether they conform to the requirements specified in SP 800-73-1. This special publication also includes detailed test assertions³ 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 800-73-1; (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 800-73-1.

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 800-73-1, SP 800-76, and SP 800-78. This special publication also includes detailed test assertions that provide the procedures to guide the tester in executing and managing the tests. This 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.

²Middleware 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.

³Test assertions are statements of behavior, action, or condition that can be measured or tested.

**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.

Appendix IV: Comments from the Office of Management and Budget

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D. C. 20503

January 25, 2008

Ms. Linda D. Koontz
Director
Information Management Issues
Government Accountability Office
441 G Street, SW
Washington, DC 20548

Dear Ms. Koontz:

Thank you for the opportunity to comment on the draft Government Accountability Office (GAO) report titled "Electronic Government: Additional OMB Leadership Needed to Optimize Use of Federal Employee Identification Cards" (GAO-08-292).

In the draft report, GAO made four recommendations for Office of Management and Budget (OMB) executive action. The report recommended the Director of OMB revise the agency's approach to overseeing implementation of Homeland Security Presidential Directive (HSPD-12) by taking the following four actions: (1) Establish realistic milestones for the full implementation of the infrastructure needed to best use the electronic authentication capabilities of Personal Identity Verification (PIV) cards in agencies; (2) Treat the HSPD-12 implementation as an investment by requiring each agency develop a detailed plan based on a risk-based assessment of the agency's physical and logical access control needs that supports the extent to which electronic authentication capabilities are to be implemented; (3) Require agencies to align the acquisition of PIV cards with plans for implementing their technical infrastructure to best use the card's electronic authentication capabilities; and (4) Ensure guidance is developed mapping existing physical security guidance to FIPS 201 guidance.

OMB has taken GAO's recommendations under advisement. These comments are in addition to the staff level comments previously provided to you. We offer the following comments to your recommendations in the draft report:

Recommendations 1 and 2: OMB agrees with GAO it is important to set milestones for implementing the necessary infrastructure to best use the electronic capabilities of the PIV cards. OMB also agrees agency investments supporting HSPD-12 implementation should be risk-based. However, OMB does not believe additional guidance on these issues is necessary at this time. OMB's previous guidance regarding HSPD-12 implementation required agencies to develop implementation plans¹ and provide milestones identifying when they intend to fully leverage the capabilities of PIV credentials for physical and logical access control.² In addition, OMB's

¹ OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, of August 5, 2005, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf>.

² OMB Memorandum of August 29, 2006, *Homeland Security Presidential Directive (HSPD) 12 Implementation Plan Update*, which can be found at: http://www.whitehouse.gov/omb/inforeg/hspd12/hspd12_id_08-2006.pdf.

previous guidance regarding E-Authentication³ required agencies to take a risk-based approach in developing their electronic authentication systems. It is important to note prior to the issuance of HSPD-12, agencies were verifying the identities of their employees and contractors, and issuing IDs. HSPD-12 is an additional identity authentication requirement. In addition, since agencies are beginning to implement plans for using the electronic capabilities of the credentials and are publicly updating the status of their efforts to complete background investigations and issue those credentials – two key components of their implementation plans, we feel additional guidance for agencies on the content of these plans is not necessary at this time.

Recommendation 3: With respect to the recommendation to align the acquisition of PIV cards with plans for implementing technical infrastructure, we recommend the report include recognition of the relationship between the HSPD-12 goals and objectives and agency information security programs. For example, HSPD-12 aligns with other security activities such as the requirement for agencies to develop plans for implementing two-factor authentication for remote access to federal information systems⁴. As noted above, we are currently monitoring agencies' progress by the number of credentials issued and we understand some of the agencies are already beginning to implement plans for using the electronic capabilities of the credentials.

Recommendation 4: This recommendation requests guidance be developed mapping existing physical security guidance to FIPS 201 guidance. The FIPS 201-1 Section 6⁵, dated March 2006, already defines a mapping between authentication assurance levels and PIV authentication methods, for both logical and physical access control systems. In addition, National Institute of Standards and Technology (NIST) is developing Special Publication 800-116, "A Strategy for the Use of PIV Credentials in Physical Access Control Systems (PACS)," which provides the *relationship* between Facility Security Levels and PIV authentication use case assurance levels.

In addition to our comments on the recommendations, we offer the following additional comments:

1) The standards and majority of guidance to support interoperability has been developed and multi-jurisdictional interoperability has already been demonstrated. NIST developed the FIPS 201 which defines the standard for PIV credentials, and they also developed special publications which provide additional technical requirements. Additionally, GSA developed several interface specifications, along with use cases. The following additional guidance is planned for FY2008: (1) NIST Special Publication 800-116; (2) NIST Special Publication 73-2, "Interfaces for Personal Identity Verification," and; (3) the interface specification for exchanging Identity Management System (IDMS) data. Additionally, we believe there is sufficient FISMA guidance, including guidance regarding E-authentication⁶, already available to assist agencies in determining the types of authentication capabilities to implement for logical access.

³ OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, of December 16, 2003, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.

⁴ OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, of June 23, 2006, which can be found at <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>.

⁵ FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, of March 2006, which can be found at <http://csrc.nist.gov/publications/PubsFIPS.html>.

⁶ NIST Special Publication 800-63, *Electronic Authentication Guidance*, of April 2006, which can be found at: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

See comment 1.

See comment 2.

2) OMB disagrees with statements there is no framework in place for agencies to electronically exchange status information on PIV credentials. There is existing capability to determine the validity of another agency user's credential. This capability is currently available via Certificate Revocation List, On-line Certificate Status Protocol, and Federal Bridge path validation services. For those agencies wanting to exchange richer identity content, the IDMS specification will be issued by GSA in FY2008.

See comment 3.

3) While we do not disagree some vendors may take several years to develop systems capable of reading the full Cardholder Unique Identifier (CHUID), the capability to read the full CHUID exists now. For example, readers are currently available that read the full CHUID but some system components (e.g., controllers) may need to be upgraded so they may use the full CHUID as the identifier in determining whether to grant access for an individual. Additionally, NIST is examining alternative approaches for the CHUID with the objective of maximizing operational efficiency without degrading security. Any alternative approach will be backward compatible with currently compliant cards.

See comment 4.

4) Statements that OMB does not consider HSPD-12 to be a major investment are inaccurate. OMB does not consider the process of verifying the identity of employees and contractors and issuing credentials to be a new investment.⁶ OMB has asked agencies to utilize existing resources for existing and planned investments as appropriate.

See comment 5.

5) In addition, we believe that the draft report does not adequately identify the extensive guidance already available for agencies. Several NIST publications are referenced in the draft, but OMB guidance is not adequately addressed. This guidance includes:

- OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, of December 16, 2003, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>.
- OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, of August 5, 2005, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf>.
- OMB Memorandum M-06-06, *Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12*, of February 17, 2006, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-06.pdf>.
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, of June 23, 2006, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>.
- OMB Memorandum of August 29, 2006, *Homeland Security Presidential Directive (HSPD) 12 Implementation Plan Update*, which can be found at: http://www.whitehouse.gov/omb/inforeg/hspd12/hspd12_id_08-2006.pdf.
- OMB Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, of January 11, 2007, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-06.pdf>.

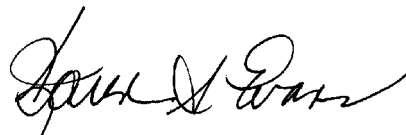
⁶ Executive Order 10450, *Security Requirements for Government Employment*, of April 27, 1953, which can be found at: <http://www.archives.gov/federal-register/codification/executive-order/10450.html>.

- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, of May 22, 2007, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>.
- OMB Memorandum M-08-01, *HSPD-12 Implementation Status*, of October 23, 2007, which can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-01.pdf>.
- OMB Memorandum of October 26, 2007, *Updated Instructions for Public Reporting of Homeland Security Presidential Directive 12 (HSPD-12) Implementation Status*, which can be found at: http://www.whitehouse.gov/omb/inforeg/hspd12/hspd-12_cio_memo_102607.pdf.

6) Lastly, we would like to clarify all agencies were required to meet the October 27, 2007 deadline for completion of background investigations for employees with 15 years or less service and all contractors. As of October 27, 2008, agencies are expected to complete background investigations for existing employees and contractors and have the capability in place to issue credentials to all new employees and contractors as part of their routine business process. Dates for completing issuance of PIV credentials to existing employees and contractors are indicated in agency/OMB mutually agreed-upon implementation plans.

We hope our comments will be reflected in GAO's final report. OMB will continue to work with departments and agencies to promote the successful implementation of the HSPD-12. As always, OMB is available to discuss its comments on GAO's draft report and to respond to questions on the Federal employee identification standard. If your staff has any questions regarding OMB's comments, please call me at 202-395-1181.

Sincerely,



Karen S. Evans

See comment 6.

GAO Comments

The following is GAO's response to the Office of Management and Budget's (OMB) additional comments.

1. We updated the report to include the additional work under way to enable interoperability.
2. We updated the report to discuss the capability of using PKI to validate credentials from other agencies. However, as we discuss in the report, procedures and specifications to enable cross-agency interoperability using the cardholder unique identifier (CHUID) have not been established. The CHUID is expected to be much more commonly used than PKI. While PIV cards and FIPS 201-compliant readers may technically be able to read the information encoded on any PIV card—including cards from multiple agencies—this functionality is not adequate to allow one agency to accept another agency's PIV card, based on reading the card's CHUID. This is because there is no common interagency framework in place for agencies to electronically exchange critical information about the card's validity, based on reading the CHUID.
3. We agree that PIV card readers currently exist that read the full CHUID. However, existing physical access control panels—which must receive and process information from the card readers—are unable to process a full CHUID. While the full CHUID is up to 27,016 bits long, most existing control panels for physical access control systems were built to process only a 26-bit identification number, and even the newest control panels are only able to process 256 bits at best.
4. We clarified the report to reflect that OMB does not consider the implementation of HSPD-12 to be a major new investment.
5. We added references to additional OMB guidance in our report.
6. Regarding OMB's comment on the implementation dates, the report notes both OMB's original deadlines and the fact that on October 23, 2007, OMB modified its guidance to indicate that agencies not meeting OMB's milestones would be directed instead to meet alternate milestones that had been mutually agreed upon by the agency and OMB.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Linda Koontz, (202) 512-6240, koontzl@gao.gov

Staff Acknowledgments

In addition to the individual named above, John de Ferrari (Assistant Director), Neil Doherty, Nancy Glover, Emily Longcore, James MacAulay, Shannin O'Neill, James Rosen, and Glenn Spiegel made key contributions to this report.

Glossary

Access Control	Process of determining the permissible activities of users and authorizing or prohibiting activities by each user.
Application Programming Interface	The interface between the application software and the application platform (i.e., operating system), across which all services are provided.
Authentication	Process of confirming an asserted identity with a specified or understood level of confidence.
Authorization	Granting the appropriate access privileges to authenticated users.
Biometric Template	A digital record of an individual's biometric features. Typically, a livenesscan of an individual's biometric attributes is translated through a specific algorithm into a digital record that can be stored in a database or on an integrated circuit chip.
Biometrics	Measures of an individual's unique physical characteristics or the unique ways that an individual performs an activity. Physical biometrics include fingerprints, hand geometry, facial patterns, and iris and retinal scans. Behavioral biometrics include voice patterns, written signatures, and keyboard typing techniques.
Card Management System	A system that 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.
Cardholder Unique Identifier	An element on the PIV card that provides for unique identification of each cardholder, specifies when the PIV card expires, and includes a digital signature capable of authenticating the card and verifying that it has not been altered.
Certificate	A digital representation of information that (1) identifies the authority issuing the certificate; (2) names or identifies the person, process, or equipment using the certificate; (3) contains the user's public key; (4) identifies the certificate's operational period; and (5) is digitally signed

by the certificate authority issuing it. A certificate is the means by which a user is linked—or bound—to a public key.

Confidentiality The assurance that information is not disclosed to unauthorized entities or computer processes.

Contactless Smart Card A smart card that can exchange information with a card reader without coming in physical contact with the reader. Contactless smart cards use 13.56 megahertz radio frequency transmissions to exchange information with card readers.

Credential An object, such as a smart card, that identifies an individual as an official representative of a government agency.

Digital Signature The result of a transformation of a message by means of a cryptographic system using digital keys, such that a relying party can determine (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate and (2) whether the message had been altered since the transformation was made. Digital signatures may also be attached to other electronic information and programs so that the integrity of the information and programs may be verified at a later time.

Electronic Credentials The electronic equivalent of a traditional paper-based credential—a document that vouches for an individual's identity.

Enrollment Station The location where an issuing agency obtains an applicant's information, including digital images of fingerprints and a digital photograph.

Identification The process of determining to what identity a particular individual corresponds.

Identity The set of physical and behavioral characteristics by which an individual is uniquely recognized.

Identity Management System	A system that stores and manages cardholder information, including the status of assigned credentials.
Identity Proofing	The process of providing sufficient information, such as identity history, credentials, and documents, to facilitate the establishment of an identity.
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged.
Logical Access Control	A mechanism for permitting or denying a user access to information and systems.
Online Certificate Status Protocol	A communications protocol that is used to determine whether a public key certificate is still valid or has been revoked or suspended.
Personal Identity Verification Card	A smart card that contains stored identity credentials—such as a photograph, digital certificate and cryptographic keys, or digitized fingerprint representations—that is issued to an individual so that the claimed identity of the cardholder can be verified against the stored credentials by another person or through an automated process.
Personal Identity Verification Card Issuer	An accredited and certified organization that procures FIPS 201-compliant blank smart cards; initializes them with the appropriate software and data elements for the requested identity verification and access control application; personalizes the cards with the identity credentials of the authorized cardholders; and delivers the personalized cards to the authorized cardholders, along with the appropriate instructions for protection and use.
Personal Identity Verification Card Registrar	An entity that authenticates an individual’s identity applying for a PIV card by checking the applicant’s identity source documents through an identity proofing process, and ensures that a proper background check is completed before the credential and the PIV card is issued to the individual.

Physical Access Control A method of permitting or denying a user access to a building or room.

Privacy The ability of an individual to control when and on what terms his or her personal information is collected, used, or disclosed.

Public Key Infrastructure A system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances—including confidentiality, data integrity, authentication, and nonrepudiation—that are important in protecting sensitive communications and transactions.

Risk The expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Smart Card A tamper-resistant security device—about the size of a credit card—that relies on an integrated circuit chip for information storage and processing.

Standard A statement published by organizations, such as NIST, the Institute of Electrical and Electronics Engineers, the International Organization for Standardization, and others, on a given topic—specifying the characteristics that are usually measurable and must be satisfied to comply with the standard.

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, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

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