United States Government Accountability Office

GAO

Report to the Chairman, Committee on Government Reform, House of Representatives

February 2006

ELECTRONIC GOVERNMENT

Agencies Face Challenges in Implementing New Federal Employee Identification Standard

G A O
Accountability ★ Integrity ★ Reliability

GAO-06-178

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-06-178, a report to the Chairman, Committee on Government Reform, House of Representatives

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 directed the establishment of a governmentwide standard—Federal Information Processing Standard (FIPS) 201—for secure and reliable forms of ID based on "smart cards" that use integrated circuit chips to store and process data with a variety of external systems across government. GAO was asked to determine (1) actions that selected federal agencies have taken to implement the new standard and (2) challenges that federal agencies are facing in implementing the standard.

What GAO Recommends

GAO recommends that the Director, OMB monitor FIPS 201 implementation progress by, for example, (1) establishing an agency reporting process to fulfill its role of ensuring FIPS 201 compliance and (2) amending or supplementing guidance to provide more complete direction to agencies on how to address implementation challenges. With the exception of OMB, which disagreed with GAO's second recommendation, agency officials generally agreed with the content of this report.

www.gao.gov/cgi-bin/getrpt?GAO-06-178.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Linda Koontz at (202) 512-6249 or koontzl@gao.gov.

February 2006

ELECTRONIC GOVERNMENT

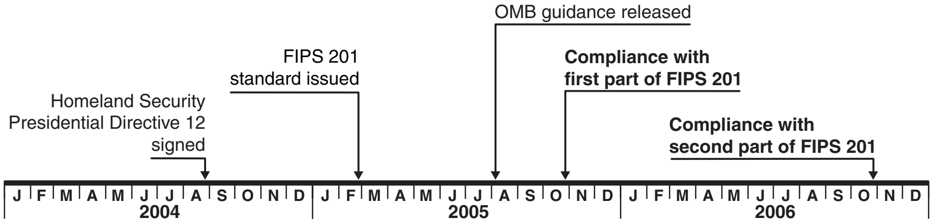
Agencies Face Challenges in Implementing New Federal Employee Identification Standard

What GAO Found

The six agencies we reviewed—Defense, Interior, Homeland Security, Housing and Urban Development (HUD), Labor, and the National Aeronautics and Space Administration (NASA)—had each taken actions to begin implementing the FIPS 201 standard. Their primary focus has been on actions to address the first part of the standard, which calls for establishing appropriate identity proofing and card issuance policies and procedures and which the Office of Management and Budget (OMB) required agencies to implement by October 27, 2005. Agencies had completed a variety of actions, such as instituting policies to require that at least a successful fingerprint check be completed prior to issuing a credential. Regarding other requirements, however, efforts were still under way. For example, Defense and NASA reported that they were still modifying their background check policies. Based on OMB guidance, agencies have until October 27, 2006, to implement the second part of the standard, which requires them to implement interoperable smart-card based ID systems. Agencies have begun to take actions to address this part of the standard. For example, Defense and Interior conducted assessments of technological gaps between their existing systems and the infrastructure required by FIPS 201 but had not yet developed specific designs for card systems that meet FIPS 201 interoperability requirements.

The federal government faces significant challenges in implementing FIPS 201, including (1) testing and acquiring compliant commercial products—such as smart cards and card readers—within required time frames; (2) reconciling divergent implementation specifications; (3) assessing the risks associated with specific vendor implementations of the recently chosen biometric standard; (4) incomplete guidance regarding the applicability of FIPS 201 to facilities, people, and information systems; and (5) planning and budgeting with uncertain knowledge and the potential for substantial cost increases. Until these implementation challenges are addressed, the benefits of FIPS 201 may not be fully realized. Specifically, agencies may not be able to meet implementation deadlines established by OMB, and more importantly, true interoperability among federal government agencies' smart card programs—one of the major goals of FIPS 201—may not be achieved.

Time Line of FIPS 201-Related Activities



Source: GAO analysis of FIPS 201 guidance.

Contents

Appendixes

Figures

Abbreviations

BLM	Bureau of Land Management
CAC	Common Access Card
DHS	Department of Homeland Security
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
GSA	General Services Administration
GSC-IS	Government Smart Card Interoperability Specification
HSPD-12	Homeland Security Presidential Directive 12
HUD	Housing and Urban Development
IAB	Smart Card Interagency Advisory Board
ID	Identification
NACI	National Agency Check with Written Inquiries
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIN	Personal Identification Number
PIV	personal identity verification
PKI	public key infrastructure

GAO
Accountability ★ Integrity ★ Reliability

United States Government Accountability Office
Washington, D.C. 20548

February 1, 2006

The Honorable Tom Davis
Chairman
Committee on Government Reform
House of Representatives

Dear Mr. Chairman:

As you know, wide variations exist in the quality and security of forms of identification (ID) used to gain access to 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 identification for federal government employees and contractors that access government-controlled facilities and information systems.

In February 2005, the National Institute of Standards and Technology (NIST) issued the required standard, titled the Federal Information Processing Standards (FIPS) Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors. Known as FIPS 201, the standard is divided into two parts. The first part, PIV-I, sets out uniform requirements for identity proofing—verifying the identity of individuals applying for official agency credentials—as well as 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 based on interoperable[1] smart cards.[2] Agencies are required by OMB to begin issuing credentials that meet these provisions

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

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

by October 27, 2006. Subsequent publications from NIST and the General Services Administration (GSA) provided supplemental guidance on various aspects of FIPS 201, including an outline of two alternate approaches that agencies may take to comply with the standard, depending on their previous experience with smart cards. Smart cards offer the potential to enhance security by significantly improving the process of authenticating the identity of people accessing federal buildings and computer systems, especially when these cards are used in combination with other technologies, such as biometrics.[3]

This report responds to your request that we conduct a review of agencies' progress in implementing systems that conform to the new federal identity card standard, as directed by HSPD-12. Specifically, our objectives were to determine (1) actions that selected federal agencies have taken to implement systems, based on the new standard and (2) challenges that federal agencies are facing in implementing such systems.

To address these objectives, we selected six agencies with a range of experience in implementing smart card-based identification systems—the Departments of Defense, Interior, Homeland Security (DHS), Housing and Urban Development (HUD), Labor, and the National Aeronautics and Space Administration (NASA). To obtain information on the actions these agencies have taken and plan to take to implement the standard, we analyzed documentation such as agencies' implementation plans and interviewed their officials. To identify challenges and barriers associated with implementing the new federal ID standard, we obtained and analyzed documentation and interviewed officials from these agencies as well as from GSA, NIST, OMB and the Office of Personnel Management (OPM). We performed our work at Defense, Interior, DHS, HUD, Labor, NASA, NIST, OMB, OPM and GSA in the Washington, D.C., metropolitan area from April 2005 to December 2005, in accordance with generally accepted government auditing standards. Further details of our objectives, scope, and methodology are provided in appendix I.

[3] A biometric measures a person's unique physical characteristics (such as fingerprints, hand geometry, facial patterns, or iris and retinal scans) or behavioral characteristics (voice patterns, written signatures, or keyboard typing techniques) and can be used to recognize the identity, or verify the claimed identity, of an individual.

Results in Brief

The six agencies that we reviewed—Defense, Interior, DHS, HUD, Labor, and NASA—have each taken actions to begin implementing the FIPS 201 standard. Their primary focus has been on actions to address the first part of the standard, which calls for establishing appropriate identity proofing and card issuance policies and procedures. For example, five of the six agencies had instituted policies to require that at least a successful fingerprint check be completed prior to issuing a credential, and the sixth agency, Defense, was in the process of having such a policy instituted. Regarding other requirements, however, efforts were still under way. For example, Defense and NASA reported that they were making modifications to their background check policies. Four of the six agencies were still updating their policies and procedures or gaining formal agency approval for them. Labor and HUD officials had completed modifications of their policies and gained approval for their PIV-I processes. Agencies have begun to take actions to address the second part of the standard, which focuses on interoperable smart card systems. Defense and Interior conducted assessments of technological gaps between their existing systems and the infrastructure required by FIPS 201, for example, but had not yet developed specific designs for card systems that meet FIPS 201 interoperability requirements.

The federal government faces a number of challenges in implementing FIPS 201, including the following:

- Testing and acquiring compliant smart cards, card readers, and other related commercial products may not be completed within OMB-mandated deadlines.

- Divergent agency implementations based on the two alternate approaches outlined in NIST guidance may delay governmentwide smart card interoperability.

- Agencies may face difficulties assessing the risks associated with specific vendor implementations of the recently chosen biometric standard.

- Incomplete guidance from OMB regarding the applicability of FIPS 201 to facilities, people, and information systems may make it difficult for agencies to meet FIPS 201 identity proofing and registration requirements consistently and economically. Existing guidance, for example, does not address significant categories of individuals, such as foreign nationals, who may need access to federal facilities and systems.

- Planning and budgeting for FIPS 201 compliance with uncertain knowledge may make it difficult for agencies to prepare accurate business cases and may affect the overall implementation schedule and planned performance of smart card investments across government agencies. For example, agencies have not had reliable information about product costs and cost elements, which are necessary for cost-benefit analyses.

Until these implementation challenges are addressed, the benefits of FIPS 201 may not be fully realized. Specifically, agencies may not be able to meet implementation deadlines established by OMB, and more importantly, true interoperability among federal government agencies' smart card programs—one of the major goals of FIPS 201—may not be achieved.

To better ensure that the objectives of HSPD-12 are met, we are recommending that the Director, OMB, take steps to closely monitor agency implementation progress and the completion of key activities by, for example, (1) establishing an agency reporting process to fulfill its role of ensuring that agencies are in compliance with the goals of HSPD-12 and (2) amending or supplementing governmentwide guidance regarding compliance with the FIPS 201 standard to provide more complete direction to agencies on how to address implementation challenges.

We received written comments on a draft of this report from the Administrator of E-Government and Information Technology of OMB, the Acting Associate Administrator of GSA, and the Deputy Secretary of Commerce. Letters from these agencies are reprinted in appendixes III through V. We received technical comments from the Director of the Access Card Office for Defense and, a Special Agent at OPM, via email, which we incorporated as appropriate. We also received written technical comments from the Assistant Secretary for Administration for HUD and the Assistant Secretary of Policy, Management, and Budget at the Interior. Additionally, representatives from NASA and Labor indicated via email that they reviewed the draft report and did not have any comments. Officials from Homeland Security did not respond to our request for comments. Officials from GSA, Commerce, HUD, Defense, Interior, and OPM generally agreed with the content of our draft report and our recommendations and provided updated information and technical comments, which have been incorporated where appropriate. OMB agreed with our recommendation on monitoring agency progress but disagreed with our recommendation on amending or supplementing government-wide policy guidance, stating that it did not think its guidance was incomplete. However, we believe OMB has not provided agencies with adequate guidance about when and how to apply the standard for important categories of individuals and facilities and for assessing risks associated with vendor implementations of the recently chosen biometric standard.

Background

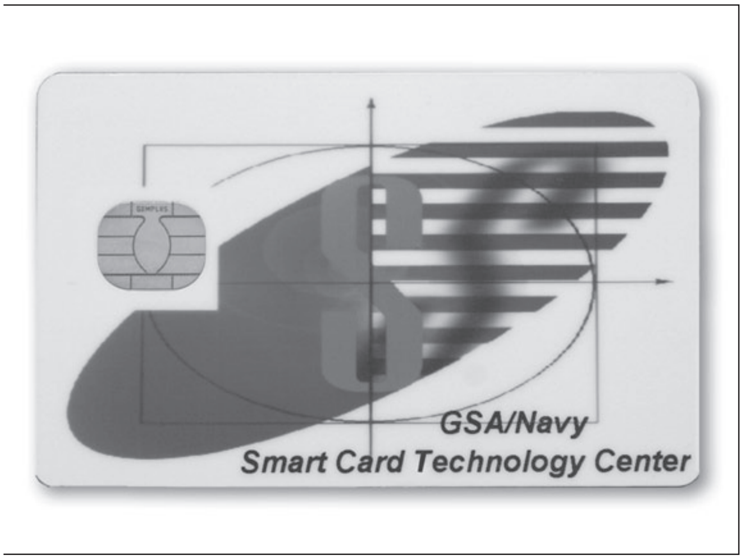
Today, federal employees are issued a wide variety of ID cards that are used to access federal buildings and facilities, sometimes solely on the basis of visual inspection by security personnel. These cards generally cannot be used to control access to an agency's computer systems. Furthermore, many can be easily forged or stolen and altered to permit access by unauthorized individuals. The ease with which traditional ID cards can be forged has contributed to increases in identity theft and related security and financial problems for both individuals and organizations. One means to address such problems is offered by the use of smart cards.

What Are Smart Cards?

Smart cards are plastic devices about the size of a credit card that 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 like magnetic stripes 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 a typical example of a smart card.

[4] The term "smart card" also may 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 widely used for services such as prepaid telephone service or satellite television reception.

Figure 1: A Typical Smart Card



Source: GSA.

Smart cards can also be used to significantly enhance the security of an organization's computer systems by tightening controls over user access. A user wishing to log on to a computer system or network with controlled access must "prove" his or her identity to the system—a process called authentication. Many systems authenticate users merely by requiring them to enter secret passwords. This 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 also 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 provides what security experts call “three-factor” authentication, the three factors being “something you possess” (the smart card), “something you know” (the password), and “something you are” (the biometric). Systems employing three-factor authentication are considered to provide a relatively high level of security. The combination of smart cards and biometrics can provide equally strong authentication for controlling access to physical facilities.[5]

Smart cards can also be used in conjunction with public key infrastructure (PKI) technology to better secure electronic messages and transactions.[6] A properly implemented and maintained PKI can offer several important security services, including assurance that (1) the parties to an electronic transaction are really who they claim to be, (2) the information has not been altered or shared with any unauthorized entity, and (3) neither party will be able to wrongfully deny taking part in the transaction. PKI systems are based on cryptography and require each user to have two different digital “keys”: a public 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.

In addition to enhancing security, smart cards have the flexibility to support a wide variety of uses not related to security, such as tracking itineraries for travelers, linking to immunization or other medical records, or storing cash value for electronic purchases. Currently, a typical smart

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

[6] PKI is a system of computers, software, and data that relies on certain cryptographic techniques for some aspects of security. For more information, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001).

card can store and process up to 32 kilobytes of data, however newer cards have been introduced that can accommodate 64 kilobytes. The larger a card's electronic memory, the more functions it can support.

Smart cards are grouped into two major classes: "contact" cards and "contactless" cards. Contact cards have gold-plated contacts that connect directly with the read/write heads of a smart card reader when the card is inserted into the device. Contactless cards contain an embedded antenna and work when the card is waved within the magnetic field of a card reader or terminal. Contactless cards are better suited to environments that require quick interaction between the card and the reader, such as places with a high volume of people seeking physical access. For example, the Washington Metropolitan Area Transit Authority has deployed an automated fare collection system using contactless smart cards as a way of speeding patrons' access to the Washington, D.C., subway system. Smart cards can be configured to include both contact and contactless capabilities, but two separate interfaces are needed because standards for the technologies are very different.

Governmentwide Smart Card Efforts Were Under Way Prior to HSPD-12

Since the 1990s, the federal government has promoted the use of smart card technology as one option for improving security over buildings and computer systems.[7] In 1996, OMB, which has statutory responsibility to develop and oversee policies, principles, standards, and guidelines—used by agencies for ensuring the security of federal information and systems—tasked GSA with taking the lead in facilitating a coordinated interagency management approach for the adoption of smart cards across government.

Because the value of a smart card is greatly enhanced if it can be used with multiple systems at different agencies, GSA worked with NIST and smart card vendors to develop the Government Smart Card Interoperability Specification, which defined a uniform set of commands and responses for smart cards to use in communicating with card readers. This specification defined a software interface for smart card systems that served to bridge the significant incompatibilities among vendors' proprietary systems. Vendors could meet the specification by writing software for their cards that translated their unique command and response formats to the

[7] For more information about previous smart card efforts, see GAO, *Electronic Government: Progress in Promoting Adoption of Smart Card Technology,* GAO-03-144 (Washington, D.C.: Jan. 3, 2003).

government standard. NIST completed the first version of the interoperability specification in August 2000. However, this and subsequent versions did not fully define all implementation details, and therefore the extent to which systems using the specification could interoperate was limited.

In 2003, OMB created the Federal Identity Credentialing Committee to make policy recommendations and develop the Federal Identity Credentialing component of the Federal Enterprise Architecture[8] to include processes such as identity proofing and credential management. In February 2004, the Federal Identity Credentialing Committee issued the Government Smart Card Handbook on the use of smart card–based systems in badge, identification, and credentialing systems with the objective of helping agencies plan, budget, establish, and implement identification and credentialing systems for government employees and their agents.

In September 2004,[9] we reported that nine agencies were planning or implementing agencywide smart card initiatives. Some of these initiatives included the Defense's Common Access Card (CAC), which had 3.2 million cards in use at the time of our review, and the Department of State's Domestic Smart Card Access Control project, which had issued 25,000 cards as of September 2004.

HSPD-12 Requires Standardized Agency ID and Credentialing Systems

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

- based on sound criteria for verifying an individual employee's identity;
- strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

[8] The Federal Enterprise Architecture is intended to provide a governmentwide framework to guide and constrain federal agencies' enterprise architectures and information technology investments.

[9] GAO, *Electronic Government: Federal Agencies Continue to Invest in Smart Card Technology*, GAO-04-948 (Washington, D.C.: Sept. 2004).

- rapidly authenticated electronically; and
- issued only by providers whose reliability has been established by an official accreditation process.

The directive stipulated that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. In addition, the directive required agencies to implement 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, to the maximum extent practicable, by October 27, 2005.[10]

NIST, OMB, and GSA Have Issued Guidance for Implementing HSPD-12

In response to HSPD-12, NIST published FIPS 201, titled “Personal Identity Verification of Federal Employees and Contractors” on February 25, 2005. The standard specifies the technical requirements for personal identity verification (PIV) systems to issue secure and reliable identification 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 the primary component of the envisioned PIV system.

The FIPS 201 standard is composed of two parts. The first part, 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. OMB directed agencies to implement the first two requirements by October 27, 2005, but did not require agencies to implement the privacy provisions until they start issuing FIPS 201 compliant identity cards, which is not expected until October 2006.

To verify individuals’ identities, agencies are required to adopt an accredited[11] identity proofing and registration process that is approved by the head of the agency and includes

[10] In August 2005, OMB issued additional guidance to agencies clarifying which elements of the standard needed to be implemented by October 27, 2005.

[11] NIST’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 organization providing its PIV card issuing services.

- initiating or completing a background investigation, such as a National Agency Check with Written Inquiries (NACI), or ensuring that one is on record for all employees and contractors;

- conducting and adjudicating a Federal Bureau of Investigation (FBI) National Criminal History Fingerprint Check (fingerprint check) for all employees and contractors prior to credential issuance;[12]

- requiring applicants to appear in person at least once before the issuance of a PIV card;

- requiring applicants to provide two original forms of identity source documents from an OMB-approved list of documents; and

- ensuring that no single individual has the capability to issue a PIV card without the cooperation of another authorized person (separation of duties principle).

Agencies are further required to adopt an accredited card issuance and maintenance process that is approved by the head of the agency and includes standardized specifications for printing photographs, names, and other information on PIV cards; loading relevant electronic applications into a card's memory; capturing and storing biometric and other data; issuing and distributing digital certificates; and managing and disseminating certificate status information. The process must satisfy the following requirements:

- ensure complete and successful adjudication of background investigations required for federal employment and revoke PIV cards if the results of investigations so justify;

- when issuing a PIV card to an employee or contractor, verify that the individual is the same as the applicant approved by the appropriate authority; and

- issue PIV cards only through accredited systems and providers.

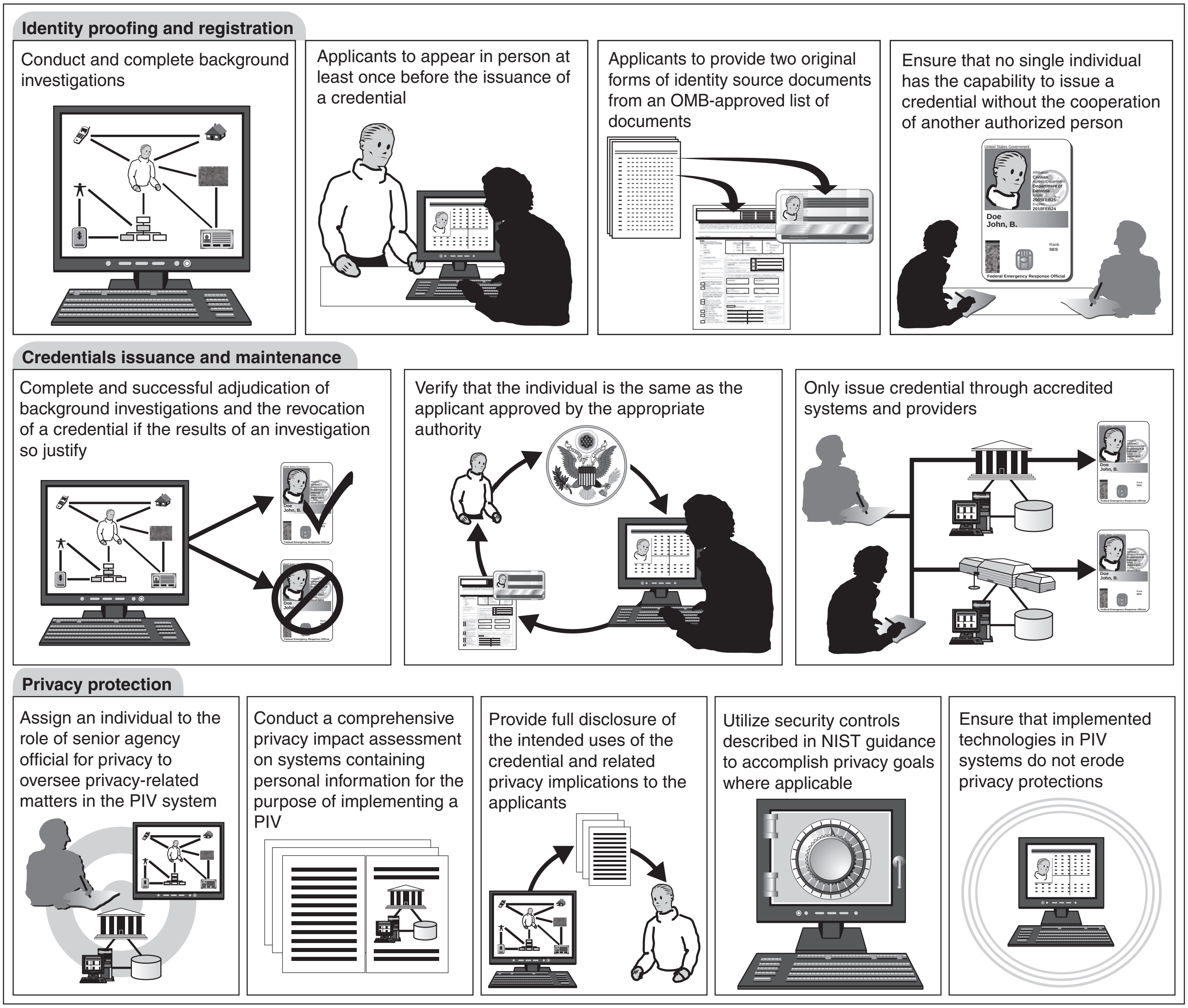
[12] In its August memorandum, OMB modified this requirement to state that if a National Agency Check is not completed within 5 days, the identity credential can be issued based solely on a FBI National Criminal History Check (fingerprint check).

Finally, agencies are required to perform the following activities to protect the privacy of the applicants, including

- assigning an individual to the role of senior agency official for privacy to oversee privacy-related matters in the PIV system,
- conducting a comprehensive privacy impact assessment on systems containing personal information for the purpose of implementing a PIV system,
- providing full disclosure of the intended uses of the PIV card and related privacy implications to the applicants,
- utilizing security controls described in NIST guidance to accomplish privacy goals where applicable, and
- ensuring that implemented technologies in PIV systems do not erode privacy protections.

Figure 2 illustrates PIV-I provisions for identity proofing and registration, card issuance and maintenance, and protection of applicants' privacy.

Figure 2: Major Provisions of PIV-I



Identity proofing and registration

Conduct and complete background investigations

Applicants to appear in person at least once before the issuance of a credential

Applicants to provide two original forms of identity source documents from an OMB-approved list of documents

Ensure that no single individual has the capability to issue a credential without the cooperation of another authorized person

Credentials issuance and maintenance

Complete and successful adjudication of background investigations and the revocation of a credential if the results of an investigation so justify

Verify that the individual is the same as the applicant approved by the appropriate authority

Only issue credential through accredited systems and providers

Privacy protection

Assign an individual to the role of senior agency official for privacy to oversee privacy-related matters in the PIV system

Conduct a comprehensive privacy impact assessment on systems containing personal information for the purpose of implementing a PIV

Provide full disclosure of the intended uses of the credential and related privacy implications to the applicants

Utilize security controls described in NIST guidance to accomplish privacy goals where applicable

Ensure that implemented technologies in PIV systems do not erode privacy protections

Source: GAO analysis of FIPS 201 guidance (data), Copyright 1997 Corel Corp. All rights reserved.

The second part of the FIPS 201 standard, PIV-II, provides technical specifications for interoperable smart card-based PIV systems. Agencies are required to begin issuing credentials that meet these provisions by October 27, 2006. The requirements 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;[13]
- physical characteristics of PIV cards, including requirements for both contact and contactless interfaces and the ability to pass certain durability tests;
- mandatory information that is to appear on the front and back of the cards, such as a photograph, the full name, card serial number and issuer identification; and
- technical specifications for electronic identity credentials (i.e., smart cards) to support a variety of authentication mechanisms, including PINs, PKI encryption keys and corresponding digital certificates, biometrics (specifically, representations of two fingerprints), and unique cardholder identifier numbers.

As outlined in a NIST special publication,[14] agencies can choose between two alternate approaches to become FIPS 201 compliant, depending on their previous experience with smart cards. The guidance sets different specifications for each approach. One approach is to adopt "transitional" card interfaces, based on the Government Smart Card Interoperability

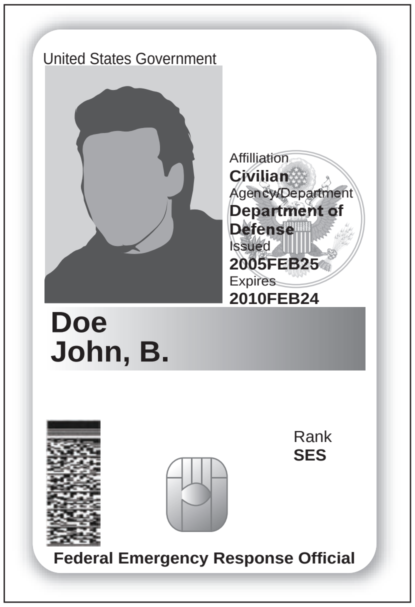
[13] The PIV assurance levels are (a) some confidence, (b) high confidence, and (c) very high confidence in authenticating the identity of PIV cardholders. For example, authentication mechanisms such as biometric and PKI technology could be implemented to provide a high or very high confidence level of assurance for physical access to federal facilities.

[14] NIST, *Interfaces for Personal Identity Verification*, Special Publication 800-73 (April 2005).

Specification (GSC-IS). Federal agencies that have already implemented smart card systems based on the GSC-IS can elect to adopt the transitional card interface specification to meet their responsibilities for compliance with part II of the standard. The other approach is to immediately adopt the "end-point" card interfaces, which are fully compliant with the FIPS 201 PIV-II card standard. All agencies without previous large scale smart card implementations are expected to proceed with implementing PIV systems that meet the end-point interface specification.

Figure 3 shows an example of a FIPS 201 card.

Figure 3: Example of a FIPS 201 Card Showing Major Required Features



Source: GAO analysis of FIPS 201 guidance (data), Copyright 1997 Corel Corp. All rights reserved.

NIST has issued several other special publications providing 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 technical specifications for implementing the required encryption technology. Additional information on NIST's special publications is provided in appendix II.

In addition, NIST was responsible for developing a suite of tests to be used by approved commercial laboratories in validating whether commercial products for the smart card and the card interface are in conformance with FIPS 201. NIST developed the test suite and designated several laboratories as interim NIST PIV Program testing facilities in August 2005. The designated facilities were to use the NIST test suite to validate commercial products required by FIPS 201 so that they could be made available for agencies to acquire as part of their PIV-II implementation efforts. According to NIST, during the next year, these laboratories will be assessed for accreditation for PIV testing. Once accreditation is achieved, the "interim" designation will be dropped.

OMB is responsible for ensuring that agencies comply with the standard, and in August 2005, it 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 below, 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. Implementation of the privacy requirements of PIV-I was deferred until agencies are ready to start issuing FIPS 201 credentials.

- *October 27, 2006*—start issuing cards that comply with the second part (PIV-II) of the standard. Agencies may defer implementing the biometric requirement until the NIST guidance is final.

- *October 27, 2007*—verify and/or complete background investigations for all current employees and contractors (Investigations of individuals who have been employees for more than 15 years may be delayed past this date.)

- *October 27, 2008*—complete background investigations for all individuals who have been federal agency employees for over 15 years. OMB guidance also includes specific time frames in which NIST and GSA must provide additional guidance, such as technical references and *Federal Acquisition Regulations*.

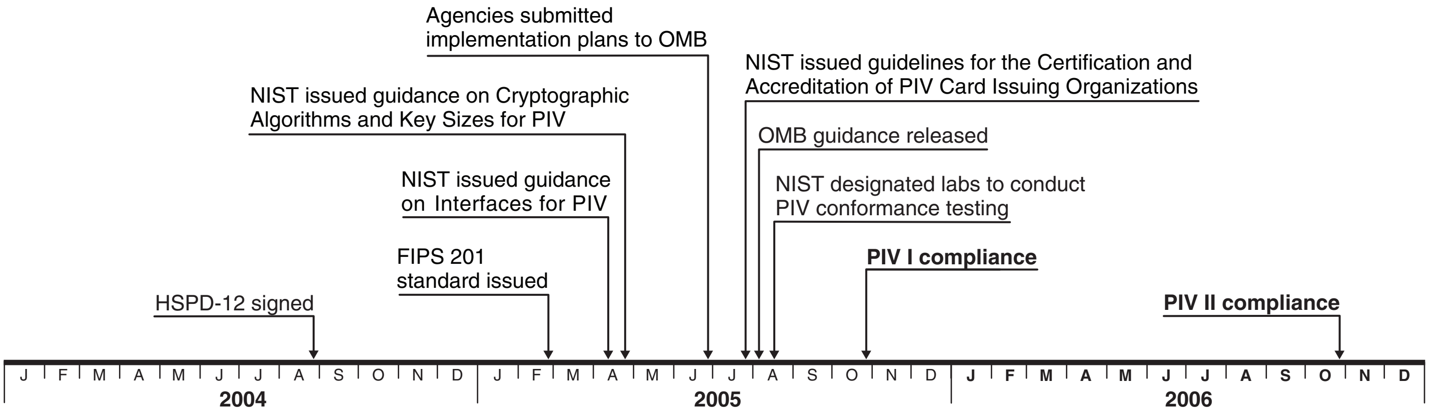
GSA, in collaboration with the Federal Identity Credentialing Committee, the Federal Public Key Infrastructure Policy Authority, OMB, and the Smart

Card Interagency Advisory Board—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 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 draft version of the handbook was released in September 2005.

In addition, on August 10, 2005, GSA issued a memorandum to agency officials that specified standardized procedures for acquiring FIPS 201-compliant commercial products that have passed NIST's conformance tests. According to the GSA guidance, agencies are required to use these standardized acquisition procedures when implementing their FIPS 201 compliant systems.

Figure 4 is a time line that illustrates when FIPS 201 and additional guidance were issued as well as the major deadlines for implementing the standard.

Figure 4: Time Line of FIPS 201 Related Activities



Agencies submitted implementation plans to OMB
NIST issued guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
NIST issued guidance on Cryptographic Algorithms and Key Sizes for PIV
OMB guidance released
NIST issued guidance on Interfaces for PIV
NIST designated labs to conduct PIV conformance testing
FIPS 201 standard issued
PIV I compliance
HSPD-12 signed
PIV II compliance
J F M A M J J A S O N D
2004
J F M A M J J A S O N D
2005
J F M A M J J A S O N D
2006

Source: GAO analysis of FIPS 201 guidance.

Agencies Have Taken Actions to Begin Implementing FIPS 201

The six agencies that we reviewed—Defense, Interior, DHS, HUD, Labor, and NASA—have each taken actions to begin implementing the FIPS 201 standard. Their primary focus has been on actions to address the first part of the standard, including establishing appropriate identity proofing and card issuance policies and procedures.[15] For example, five of the six agencies had instituted policies to require that at least a successful fingerprint check be completed prior to issuing a credential; and the sixth agency, Defense, was in the process of having such a policy instituted. Regarding other requirements, efforts were still under way. For example, Defense and NASA reported that they were still making modifications to their background check policies. Four of the six agencies were still updating their policies and procedures or gaining formal agency approval for them. Labor and HUD officials had completed modifications of their policies and gained approval for their PIV-I processes.

Agencies have begun to take actions to address the second part of the standard, which focuses on interoperable smart card systems. Defense and Interior, for example, have conducted assessments of technological gaps between their existing systems and the infrastructure required by FIPS 201, but they have not yet developed specific designs for card systems that meet FIPS 201 interoperability requirements.

Department of Defense

Defense has been working on implementing smart card technology since 1993, when the Deputy Secretary of Defense issued a policy directive that called for the implementation of the CAC program, a standard smart card-based identification system for all active duty military personnel, civilian employees, and eligible contractor personnel. Defense began testing the CAC in October 2000 and started to implement it departmentwide in November 2001.

Currently, the CAC program is the largest smart card deployment within the federal government, with approximately 3.8 million cards considered active or in use as of May 2005. The CAC addresses both physical and logical access capabilities and incorporates PKI credentials.

[15] The specific requirements for the first part of the standard (PIV-I) are outlined earlier in this report.

Defense officials have taken steps to implement PIV-I requirements but have not yet completed all planned actions. For example, according to agency officials, Defense implemented its first PIV-I compliant credential issuance station, accredited and trained designated individuals to issue credentials, and took steps to better secure access to Defense personnel data. However, at the time of our review, Defense was still drafting modifications to the department's background check policy to meet PIV-I requirements, and agency officials expected to issue a revised policy by the end of December 2005. Work was also under way to modify an automated system used by contractors to apply for the CAC to comply with the PIV-I background check requirements for contractors.

To address PIV-II, Defense program officials conducted an assessment to identify the technological gaps between their existing CAC infrastructure and the infrastructure required to meet PIV-II interoperability requirements. This assessment identified that of the 245 requirements specified by FIPS 201, the CAC did not support 98 of those requirements, which led to a strategy to implement each of the needed changes. Some of the changes include deploying cards that contain both contact and contactless capabilities; ensuring that information on the cards is in both visual and electronic form; and ensuring that the electronic credentials stored on PIV cards to verify a cardholder's identity contain all required data elements, including the cardholder's PIN, PIV authentication data (PKI encryption keys and corresponding digital certificates), and two fingerprints. Additionally, program officials prepared rough cost estimates for specific elements of their planned implementation, such as cards and card readers. Program officials have also begun developing agency-specific PIV applications to be stored on the cards. However, Defense has not yet developed a specific design for a card system that meets FIPS 201 interoperability requirements.

Department of the Interior

In January 2002, Interior's Bureau of Land Management (BLM) launched a smart card pilot project to help improve security over its sites and employees. About 2,100 employees were given smart cards for personal ID and for access to sites in the pilot program.

Having successfully implemented the smart card pilot at BLM, Interior began a program to implement smart cards agencywide. According to program officials, the agencywide smart card system is in compliance with the GSC-IS specification. As of October 19, 2005, the department had deployed approximately 20,000 smart cards, providing access control for approximately 25 buildings.

Interior officials have taken steps to implement PIV-I requirements but have not yet had their system accredited or approved, as required by the standard. For example, Interior revised its policy on identity proofing and registration to require at least a fingerprint check be completed before issuing a credential. Regarding card issuance and maintenance processes, Interior revised its policies to include steps to ensure the completion and successful adjudication of a NACI or equivalent background investigation for all employees and contractor personnel. Additionally, Interior officials reported they had completed more than 90 percent of all required background checks for existing employees, and had signed a contract to develop a Web-enabled PIV-I identity proofing and registration process, which may eventually replace the current manual process. However, as of November 2005, Interior's identity proofing, registration, issuing, and maintenance processes had not been accredited or approved by the head of the agency. Regarding privacy protection, according to the officials, they had completed two privacy impact assessments on systems containing personal information for the purposes of implementing PIV-I.

To meet PIV-II requirements, Interior officials reported that they had established a pilot PKI and had also conducted a gap analysis to identify specific areas in which their existing smart card system does not meet the FIPS 201 standard. In the absence of approved FIPS 201 compliant products, they had not developed a specific design for a card system that meets FIPS 201 interoperability requirements.

Department of Homeland Security

Prior to the issuance of FIPS 201, DHS developed a smart card-based identification and credentialing pilot project that was intended to serve as a comprehensive identification and credentialing program for the entire department when fully deployed. This effort was based on the GSC-IS specification and was intended to use PKI technology for logical access and proximity cards that are read by electronic readers to gain building access. As of November 2005, program officials indicated that they had deployed approximately 150 cards as part of this effort. However, OMB directed DHS to not issue smart cards until it had developed and implemented a system based on cards that are fully compliant with the PIV-II section of FIPS 201.

DHS officials have taken steps to implement PIV-I requirements but, as of November 2005, were still making necessary modifications to their policies and procedures. For example, DHS revised its policy on identity proofing and registration to require at least a fingerprint check be completed before issuing a credential.

However, other DHS actions to implement PIV-I were still under way. For example, according to DHS officials, they had not yet fully implemented the requirements to ensure that background checks are successfully adjudicated or to establish a credential revocation process. DHS officials further stated that they were finalizing a security announcement that would outline the PIV-I process.

DHS officials had begun to take actions to meet PIV-II requirements. According to program officials, to help plan and prepare the agency for deployment, they conducted a survey of all DHS components to determine the types of information systems their various components had deployed. However, officials have planned to wait until approved FIPS 201 products and services are available before purchasing any equipment or undergoing any major deployment of a PIV-II compliant system.

National Aeronautics and Space Administration

NASA officials indicated that they had been working to improve their identity and credentialing process since 2000. Prior to the issuance of FIPS 201, NASA officials were planning for the implementation of the One NASA Smart Card Badge project. This project was intended to be deployed agencywide and was being designed to provide GSC-IS compliant smart cards for identity, physical access, and logical access to computer systems. However, NASA officials were directed by OMB to not implement this system because it had not initiated large-scale deployment of its smart cards prior to July 2005. In the meantime, NASA has been utilizing proximity cards,[16] which are read by electronic readers, to gain building access.

NASA officials have taken steps to implement PIV-I requirements; but, as of November 2005, they were still making necessary modifications to their policies and procedures. For example, regarding identity proofing and registration, NASA officials stated that they had modified their policy to address the fingerprint check requirement. According to NASA officials, they have also implemented a process for gathering all required data

[16] This is a security system utilizing cards with embedded radio frequency technology.

elements from individuals, with the exception of the biometric data. In addition, NASA officials conducted an analysis of how FIPS 201 requirements impact security within NASA. Other NASA actions to implement PIV-I were still under way. For example, NASA was getting its revised policy approved which specifies the completion and successful adjudication of the NACI. Regarding privacy protection, NASA was updating its privacy impact assessments for relevant systems containing personal information for the purpose of implementing PIV-I.

NASA has begun to take actions to implement PIV-II requirements. NASA officials said they were planning to modify their existing PKI to issue digital certificates that can be used with the PIV cards that will be issued under FIPS 201. In the absence of approved FIPS 201 compliant products, NASA has not developed specific designs for a card system that meets FIPS 201 interoperability requirements.

Department of Housing and Urban Development

HUD did not have an existing smart card program in place prior to HSPD-12. Like NASA, HUD controls physical access to its buildings by using proximity cards that are read by electronic readers.

HUD officials reported that they have taken steps to implement PIV-I requirements. To meet identity proofing and registration practices, for example, officials modified their policies to require that at least a fingerprint check be completed before issuing a credential. Policies regarding card issuance and maintenance processes were also modified to ensure that all necessary steps were in place regarding the completion and successful adjudication of a NACI or another equivalent background investigation. Additionally, HUD issued guidelines explaining policies and procedures to ensure that the issuance of credentials complies with PIV-I. Program officials have also been analyzing the differences between their existing processes and those required by FIPS 201. As of January 2006, HUD's identity proofing, registration, issuing, and maintenance processes were approved by HUD's Assistant Secretary for Administration, as required by PIV-I. Finally, regarding privacy protections, officials have drafted a document describing how personal information will be collected, used, and protected throughout the lifetime of the FIPS 201 cards.

Thus far, HUD's actions related to PIV-II have been limited to analyzing their needs and planning for physical security and information technology infrastructure requirements. HUD officials said they had developed rough estimates to determine how much implementing FIPS 201 would cost. In the absence of approved FIPS 201 compliant products, HUD officials have not developed a specific design for a card system that meets FIPS 201 interoperability requirements.

Department of Labor

Like HUD, Labor did not have an existing smart card program in place prior to HSPD-12. Labor currently utilizes a nonelectronic identity card that contains an employee's photograph and identifying information. The identity cards can only be used for physical access, which is granted by security personnel once they have observed the individual's identity card.

As of November 2005, Labor officials reported that they had implemented the major requirements of PIV-I. As an example of Labor's efforts to implement identity proofing and registration requirements, the officials modified their policies to require that, at minimum, a fingerprint check is conducted and successfully adjudicated prior to issuing the credential. Regarding issuance and maintenance processes, Labor officials modified their policies to ensure all necessary steps were in place regarding the completion and successful adjudication of the NACI or another equivalent background investigation. In addition, the officials reported that they had implemented a system of tracking metrics for background investigations to ensure that they are completed and successfully adjudicated.

Labor officials stated that they had not made substantial progress toward implementing PIV-II because they were waiting for compliant FIPS 201 products to become available before making implementation decisions.

The Federal Government Faces Challenges in Implementing FIPS 201

The federal government faces a number of significant challenges to implementing FIPS 201, including testing and acquiring compliant products within OMB's mandated time frames; reconciling divergent implementation specifications; assessing risks associated with implementing the recently-chosen biometric standard; incomplete guidance regarding the applicability of FIPS 201 to facilities, people, and information systems; and planning and budgeting with uncertain knowledge and the potential for substantial cost increases. Addressing these challenges will be critical in determining whether agencies will be able to meet fast-approaching implementation deadlines and in ensuring that agencies' FIPS 201 systems are interoperable with one another.

Testing and Acquiring Compliant Products within OMB-Mandated Time Frames

Based on OMB and GSA guidance, all commercial products, such as smart cards, card readers, and related software, are required to successfully complete interdependent tests before agencies can purchase them for use in their FIPS 201 compliant systems. These tests include (1) conformance testing developed by NIST to determine whether individual commercial products conform to FIPS 201 specifications, (2) performance and interoperability testing to be developed by GSA to ensure that compliant products can work together to meet all the performance and interoperability requirements specified by FIPS 201, and (3) agencies' testing to determine whether the products will work satisfactorily within the specific system environments at each of the agencies.

Because it is difficult to predict how long each of these tests will take, and because they must be done in sequence, fully tested FIPS 201 compliant products may not become available for agencies to acquire in time for them to begin issuing FIPS 201 compliant ID cards by OMB's deadline of October 27, 2006. According to NIST officials, conformance testing of individual commercial products, based on the test suite developed by NIST, was authorized to begin on November 1, 2005. The officials indicated that it would take a minimum of several weeks to test and approve a product—assuming the product turned out to be fully FIPS 201 compliant—and would more likely take significantly longer. Experience with similar NIST conformance testing regimes, such as FIPS 140-2 cryptography testing, has shown that this process can actually take several months. According to a FIPS 140-2 consulting organization,[17] the variability in the time it takes to test products depends on (1) the complexity of the product, (2) the completeness and clarity of the vendor's documentation, (3) how fast the vendor is able to answer questions and resolve issues raised during testing, and (4) the current backlog of work encountered in the lab. According to officials from NIST and the Smart Card Alliance,[18] these factors are likely to keep FIPS 201 compliant products from completing conformance testing and becoming available for further testing until at least the early part of 2006.

[17] Corsec Security, Inc., provides consulting services to companies that are aiming to certify their products as being FIPS 140-2 compliant.

[18] According to the Smart Card Alliance, it is a not-for profit, multi-industry association working to influence standards that are relevant to smart card adoption and implementation, maintain a voice in public policy that affects smart card adoption and implementation, serve as an educational resource to its members and the industry, and provide a forum for discussions and projects on issues surrounding smart cards.

Furthermore, once commercial products pass conformance testing, they must then go through performance and interoperability testing. These tests are intended to ensure that the products meet all the performance and interoperability requirements specified by FIPS 201. According to GSA, which was developing the tests, they can only be conducted on products that have passed NIST conformance testing. GSA will also conduct performance and interoperability tests on other products that are required by FIPS 201, but not within the scope of NIST's conformance tests, such as smart card readers, fingerprint capturing devices, and software required to program the cards with employees' data. At the time of our review, GSA officials stated that they were developing initial plans for these tests and had planned to have the tests ready in March 2006. GSA officials indicated that once they finalized the tests, they estimated that it would take approximately 2 to 3 months to test each product. Officials stated that they do not expect to have multiple products approved until May 2006, at the earliest. Vendors with approved products and services will be awarded a blanket-purchase agreement, making them available for agencies to acquire. According to GSA officials, there will be a modification to the *Federal Acquisition Regulation* to require that agencies purchase PIV products through this blanket-purchase agreement.

Prior to purchasing commercial products, each agency will also need to conduct its own testing to determine how well the products will work in conjunction with the rest of the agency's systems. According to agency officials, this process could take from 1 to 8 months, depending on the size of the agency. For example, GSA officials estimated that a small agency could complete this testing in about 1 month. Defense officials, in contrast, estimated it would take them about 4 months to conduct testing, and Interior officials have stated that, based on their prior experience, it would take 6 months to conduct the testing. When Defense initially implemented their CAC system, it took 8 months to conduct testing. Following this series of tests, agencies must also acquire products—which could add at least an additional month to the process—and install them at agency facilities.

OMB, which is tasked with ensuring compliance with the standard, has not indicated how it plans to monitor agency progress in developing systems based on FIPS 201 compliant products. For example, OMB has not stated whether it will require agencies to report on the status of their FIPS 201 implementations in advance of the October 2006 deadline.

While in the best case scenario it may be possible for some agencies to purchase compliant products and begin issuing FIPS 201 compliant cards to employees by OMB's deadline of October 27, 2006, it will likely take significantly longer for many other agencies. With compliance testing scheduled to be complete in early 2006 and at least two sets of additional testing required, each of which could potentially take many months, many agencies are likely to be at risk of not meeting the deadline to begin issuing FIPS 201 compliant credentials. Given these uncertainties, it will be important to monitor agency progress and completion of key activities to ensure that the goals of HSPD-12 are being met.

Reconciling Divergent Implementation Specifications

Recognizing that some agencies, such as Defense, have significant investments in prior smart card technology that does not comply with the new standard, NIST, in supplemental guidance on FIPS 201,[19] allowed such agencies to address the requirements of FIPS 201 by adopting a "transitional" smart card approach. According to the guidance, the transitional approach should be based on the existing GSC-IS specification and should be a temporary measure prior to implementing the full FIPS 201 specification, known as the "end point" specification. Agencies without existing large-scale smart card systems were to implement only systems that fully conform to the end-point specification. NIST deferred to OMB to set time frames for when agencies adopting the transitional approach would be required to reach full compliance with the end-point specification. However, OMB has not yet set these time frames and has given no indication of how or when it plans to address this issue.

The provision for transitional FIPS 201 implementations in NIST's guidance acknowledges that agencies with fully implemented GSC-IS smart card systems may already be meeting many of the security objectives of FIPS 201 and that it may be unreasonable to require them to replace all of their cards and equipment within the short time frames established by HSPD-12. However, according to NIST officials, the transitional specification is not technically interoperable with the end-point specification. Thus, cards issued by an agency implementing a transitional system will not be able to interoperate with systems at agencies that have implemented the end-point specification until those agencies implement the end-state specification, too.

[19] NIST, *Interfaces for Personal Identity Verification*, Special Publication 800-73 (April 2005).

Although allowing for the transitional approach to FIPS 201 compliance in their guidance, NIST stated that agencies should implement the end-point specification directly, wherever possible. According to NIST, agencies that adopt the transitional specification will have to do more work than if they immediately adopt the end-point specification. Specifically, major technological differences between the two interfaces will require agencies to conduct two development efforts—one to adopt the transitional specification and then another at a later date to adopt the end-point specification.

Agencies with substantial smart card systems already deployed—such as Defense and Interior—have chosen the transitional option because they believe it poses fewer technical risks than the end-point specification, which is a new standard. These agencies do not plan to implement end-point systems by the October 2006 deadline for PIV-II compliance, nor have they determined when they will have end-point systems in place. According to OMB, these agencies will be allowed to meet OMB's October 2006 deadline by implementing the transitional specification. Defense officials stated that, based on their past experience in implementing the CAC system, they believe the transitional approach will entail fewer development problems because it involves implementing hardware and software that is similar to their current system. Further, Defense officials indicated that implementing the end-point specification would be risky. For example, Defense officials conducted a technical evaluation, which determined that the specification was incomplete. The officials stated that they would not plan to adopt the end-point specification until at least one other agency has demonstrated a successful implementation. Similarly, Interior officials said they also plan to use products based on the transitional specification until approved end-point products are readily available.

While NIST and OMB guidance on FIPS 201 compliance allows agencies to meet the requirements of HSPD-12 using two divergent specifications that lead to incompatible systems, it does not specify when agencies choosing the transitional approach need to move from that approach to the end-point specification. Until OMB provides specific deadlines for when agencies must fully implement the end-point specification, achieving governmentwide interoperability—one of the goals of FIPS 201—may not be achieved.

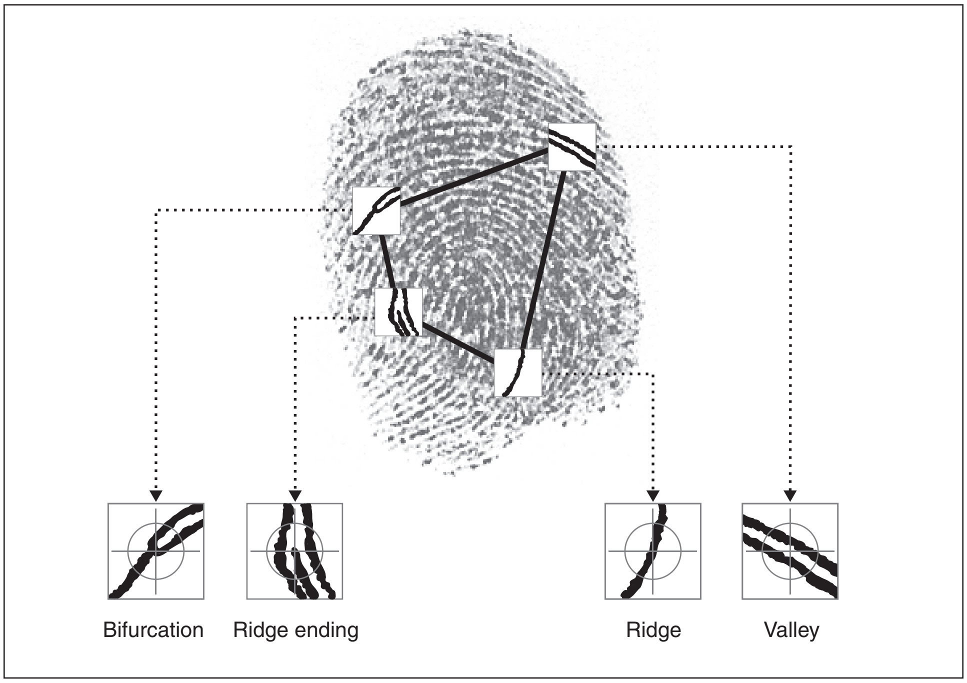
Assessing Risks Associated with Implementing the Recently-Chosen Biometric Standard

One of the major requirements of FIPS 201 is that electronic representations of two fingerprints be stored on each PIV card. In January 2005, NIST issued initial draft guidance for storing electronic images of fingerprints on PIV cards in accordance with a preexisting standard. NIST based its draft guidance on the fact that the existing fingerprint image standard is internationally recognized and thus can facilitate interoperability among multiple vendors' products.

When agency officials and industry experts reviewed and commented on the initial draft guidance, they were strongly opposed to the use of fingerprint images, arguing instead for a more streamlined approach that would take less electronic storage space on the cards and could be accessed more quickly. According to industry experts, because the large amount of memory required for images can only be accessed very slowly, it could take approximately 30 seconds for card readers to read fingerprint information from an electronic image stored on a card—a length of time that would likely cause unacceptable delays in admitting individuals to federal buildings and other facilities.

Instead of relying on electronic images, agency officials and industry experts advocated that the biometric guidance instead be changed to require the use of "templates" extracted from fingerprint "minutiae." A minutiae template is created by mathematically extracting the key data points related to breaks in the ridges of an individual's fingertip. As shown in figure 6, the most basic minutiae are ridge endings (where a ridge ends) and bifurcations (where a single ridge divides into two). Using minutiae templates allows for capturing only the critical data needed to confirm a fingerprint match, and storing just those key data points rather than a full representation of an individual's fingerprint. Thus, this technique requires much less storage space than a full electronic image of a fingerprint.

Figure 5: Common Fingerprint Feature



Source: GAO adaptation of FBI data.

An additional benefit of using minutiae templates is rapid processing capability. Because minutiae data require a much smaller amount of storage space than fingerprints in image format, the smaller data size allows for decreased transmission time of fingerprint data between the cards and the card readers—approximately 7 to 10 seconds, according to industry experts at Smart Card Alliance. Short transmission times are especially important for high traffic areas such as entrances to federal buildings.[20]

Despite these advantages, existing minutiae template technology suffers from two significant drawbacks. One disadvantage is that vendors' techniques for converting fingerprint images to minutiae are generally

[20] Agencies are not required to implement biometric authentication at all facilities. Instead, each agency must make a risk-based decision to determine where it will require the use of biometrics.

proprietary and incompatible; a minutiae template that one vendor uses cannot be used by another. Another disadvantage of template technology is its questionable reliability. Different algorithms for extracting minutiae produce templates with varying reliability in producing accurate matches with the original fingerprints.

To resolve these issues, NIST began systematically testing minutiae template algorithms submitted by 14 vendors to determine if it is possible to adopt a standard minutiae template that can accurately match templates to individuals. NIST officials anticipate that testing will be completed by February 2006, when they expect to be able to determine the accuracy and level of interoperability that can be achieved for the 14 vendors being tested, using standard minutiae templates.

In December 2005, NIST officials stated that they had conducted enough tests to determine that the reliability, accuracy, and interoperability of minutiae data among these 14 vendors were generally within the bounds of what was likely to be required for many applications of the technology. However they noted that the tests showed that the products of the 14 vendors varied significantly in their reliability and accuracy—by as much as a factor of 10. NIST officials expect that once they complete testing in February 2006, they will have sufficient data to establish the reliability and accuracy of each of the 14 vendors.

Despite the fact that the testing of minutiae template technology was still under way, NIST was requested by the Executive Office of the President to issue revised draft guidance[21] that replaced the previously proposed image standard with a minutiae standard. While the minutiae standard resolves the problems of storage and access speed associated with the image standard, it opens new questions about how agencies should choose vendor implementations of the minutiae standard, due to their varying reliability and accuracy. Agencies will need to ensure that the vendors they select to provide minutiae template matching will provide systems that provide the level of reliability and accuracy needed for their applications. Agencies will also have to determine the level of risk they are willing to accept that fingerprints may be incorrectly matched or incorrectly fail to match. According to NIST officials, agencies may find that in order to preserve interoperability across agencies' systems, they may need to allow

[21] NIST, *Biometric Data Specification for Personal Identity Verification*, Special Publication 800-76 (Draft, December 2005).

for less reliability and accuracy in determining whether fingerprints match. This reduction in reliability and accuracy—and the associated higher security risk—could pose problems for secure facilities that require very high levels of assurance. Further, according to NIST officials, any vendors beyond the 14 currently being tested would need to undergo similar testing in order to determine their levels of reliability and accuracy. If agencies do not fully understand the implications of the variation in accuracy among the biometric vendors, the security of government facilities could be compromised and interoperability between agencies could be hindered.

Incomplete Guidance Regarding the Applicability of FIPS 201 to Facilities, People, and Information Systems

FIPS 201 and OMB's related guidance provide broad and general criteria regarding the facilities, people, and information systems that are subject to the provisions of FIPS 201. For instance, according to FIPS 201, compliant identification credentials must be issued to all federal employees and contractors who require physical access to federally controlled facilities—including both federally owned buildings and leased space—and logical access to federally controlled information systems. OMB guidance adds that agencies should make risk-based decisions on how to apply FIPS 201 requirements to individuals and information systems that do not fit clearly into the specified categories. For example, OMB guidance states that applicability of FIPS 201 for access to federal systems from a nonfederally controlled facility (such as a researcher uploading data through a secure Web site or a contractor accessing a government system from its own facility) should be based on a risk determination made by following NIST guidance on security categorizations for federal information and information systems (FIPS 199).

Although this guidance provides general direction, it does not provide sufficient specificity regarding when and how to apply the standard. For example, OMB's guidance does not explain how NIST's security categories can be used to assess types of individuals accessing government systems. FIPS 199 provides guidance only on how to determine the security risk category of government information and information systems, not how such a category relates to providing access from nonfederally controlled facilities. As a result, agencies are unlikely to make consistent determinations about when and how to apply the standard. HUD is one example of an agency that has not been able to finalize how it would implement FIPS 201, with regard to allowing access to federal information systems from remote locations; and according to a HUD official, they are considering multiple options.

Further, the guidance does not address all categories of people who may need physical and logical access to federal facilities and information systems. Specifically, for individuals such as foreign nationals, volunteers, and unpaid researchers, meeting some of the FIPS 201 requirements—such as conducting a standard background investigation—may be difficult. For example, Defense and NASA employ a significant number of foreign nationals—individuals who are not U.S. citizens and work outside the U.S. foreign nationals generally cannot have their identity verified through the standard NACI process. In order to conduct a NACI, an individual must have lived in the United States long enough to have a traceable history, which may not be the case for foreign nationals. According to NASA officials, approximately 85 percent of NASA's staff at its Jet Propulsion Laboratory are foreign nationals. However, OMB's guidance for such individuals states only that agencies should conduct an "equivalent investigation," without providing any specifics that would ensure the consistent treatment of such individuals.

Specifically regarding foreign nationals, the Smart Card Interagency Advisory Board (IAB) and OMB have recognized that FIPS 201 may not adequately address this issue. The IAB obtained data from agencies who hire foreign nationals to more specifically identify the issues with identity proofing of foreign nationals. According to IAB representatives, these data were provided to OMB. In addition, OMB indicated that they planned to establish an interagency working group to assess whether additional guidance is necessary concerning background investigations for foreign nationals. However, no time frames have been set for issuing revised or supplemental guidance regarding foreign nationals.

In addition to foreign nationals, other types of workers also have not been addressed. For example, Interior has approximately 200,000 individuals that serve as volunteers, some of whom require access to facilities and information systems. OMB's guidance provides no specifics on what criteria to use to make a risk-based decision pertaining to access to facilities and systems by volunteers.

Moreover, the guidance is not clear on the extent to which FIPS 201 should be implemented at all federal facilities. While the standard provides for a range of identity authentication assurance levels based on the degree of confidence in the identity of cardholders,[22] it does not provide guidance on establishing risk levels for specific facilities or how to implement FIPS 201 based on an assessment of the risks associated with facilities. Therefore, agencies such as HUD, which has 21 field offices with five or fewer employees, and Interior, which has 2,400 field offices, many of which are also quite small, do not have the guidance necessary to make decisions consistently about how to implement FIPS 201 at each of their facilities. Depending on how risks are assessed, to implement a FIPS 201 compliant access control system at each facility could represent a significant expense, including possibly acquiring and installing card readers, network infrastructure, biometric hardware and software. As of November 2005, OMB officials reported no specific plans to supplement or revise its FIPS 201 implementation guidance to address these issues.

Without more specific and complete guidance on the scope of implementing FIPS 201 regarding individuals, facilities, and information systems, the objectives of HSPD-12 could be compromised. For instance, agencies could adopt varying and inconsistent approaches for identity proofing and issuing PIV cards to foreign nationals and volunteers needing physical and logical access to their facilities and information systems, thus undermining the objective of FIPS 201 to establish consistent processes across the government. Variations from the standard could also pose problems within each agency. Specifically, if agencies choose to make exceptions to implementing FIPS 201 requirements for specific categories of individuals, information systems, or facilities, such exceptions could undermine the security objectives of the agency's overall FIPS 201 implementation. Conversely, some agencies could expend resources implementing FIPS 201 infrastructure at locations where it is not really needed or may impose unnecessary constraints on access, due to the lack of clarity of FIPS 201 guidance.

Planning and Budgeting with Uncertain Knowledge

Agencies have been faced with having to potentially make substantial new investments in smart card technology systems with little time to adequately plan and budget for such investments and little cost information about products they will need to acquire. To comply with budget submission

[22] FIPS 201 defines three levels of assurance for identity authentication supported by the PIV card, such as the card holder unique identification number, biometrics, and PKI. Each assurance level refers to the degree of confidence established in the identity of the PIV card holder.

deadlines, agencies would have had to submit budget requests for new systems to meet the October 2006 PIV-II deadline in the fall of 2004, several months prior to the issuance of FIPS 201. If a major information technology (IT) investment were expected, agencies also would have had to submit business cases at the same time. Agencies were not in a position to prepare such documentation in the fall of 2004, nor were they able to determine whether a major new investment would be required.

As part of the annual federal budget formulation process, agencies are required to submit their budget requests 1 year in advance of the time they expect to spend the funds. In addition, in the case of major IT investments, which could include new smart-card based credentialing systems, OMB requires agencies to prepare and submit formal businesses cases, which are used to demonstrate that agencies have adequately defined the proposed cost, schedule, and performance goals for the proposed investments.[23] In order for agencies to prepare business cases for future funding requests, they need to conduct detailed analyses such as a cost-benefit analysis, a risk analysis, and an assessment of the security and privacy implications of the investment.

However, agencies have lacked the information necessary to conduct such reviews. For example, agencies have not had reliable information about product costs and cost elements, which are necessary for cost-benefit analyses. In addition, without FIPS 201 compliant products available for review, agencies have been unable to adequately conduct risk analyses of the technology. Most importantly, the lack of FIPS 201 compliant products has inhibited planning for addressing the investment's security and privacy issues.

Several officials from the agencies we reviewed reported that they based their cost estimates on experience with existing smart card systems because they could not predict the costs of FIPS 201 compliant products. For example, HUD officials reported that in order to formulate their

[23] In response to the Clinger-Cohen Act and other statutes, OMB developed section 300 ("business case") of *Circular A-11*, which provides policy for planning, budgeting, acquisition, and management of federal capital assets. This reporting mechanism, as part of the budget formulation and review process, is intended to enable an agency to demonstrate to its own management, as well as OMB, that it has employed the disciplines of good project management, developed a strong business case for the investment, and met other administration priorities in defining the cost, schedule, and performance goals proposed for the investment.

preliminary budget, they developed implementation estimates based on discussions with various vendors about similar technology as well as discussions with other agencies regarding their past experiences with smart card implementation. Furthermore, Defense and Labor officials reported that the only information they had on which to base costs was Defense's CAC—a smart card system that has significant differences from FIPS 201.

While it is not known how much FIPS 201 compliant systems will cost, OMB maintains that agencies should be able to fund their new FIPS 201 compliant systems with funds they are spending on their existing ID and credentialing systems. However, officials from agencies such as HUD—who stated that they estimate that implementing a FIPS 201 system will cost approximately 400 percent more than their existing identification system—have indicated that existing funds will be insufficient to finance implementation of the FIPS 201 system. As of November 2005, OMB officials did not report any specific plans to monitor agencies' funding of FIPS 201 compliant card systems to ensure that the systems can be implemented in a timely fashion.

As a result of the lack of cost and product information necessary for the development of accurate budget estimates, agency officials believe they may not have sufficient funds to implement FIPS 201 within the time frames specified by OMB. Further, the overall implementation schedules and planned performance of FIPS 201 investments across the government could be affected.

Conclusions

Agencies have been focusing their efforts on a range of actions to establish appropriate identity proofing and card issuance policies and procedures to meet the first part of the FIPS 201 standard. They have also begun to take actions to implement new smart card-based ID systems that will be compliant with the second part of the standard. With the deadline for implementing the second part of the standard approaching in October 2006, the government faces significant challenges in implementing the requirements of the standard.

Several of these challenges do not have easy solutions— testing and acquiring compliant smart cards, card readers, and other related commercial products within OMB-mandated deadlines; implementing fully functional systems; and planning and budgeting for FIPS 201 compliance with uncertain knowledge. OMB officials have not indicated any plans to monitor the impact on agencies of the constrained testing time frames and funding uncertainties, which could put agencies at risk of not meeting the compliance goals of HSPD-12 and FIPS 201. Without close monitoring of agency implementation progress through, for example, establishing an agency reporting process, it could be difficult for OMB to fulfill its role of ensuring that agencies are in compliance with the goals of HSPD-12.

Other challenges have arisen because guidance to agencies has been incomplete. For example, time frames have not been set for agencies implementing transitional smart card systems to migrate to the fully compliant end-point specification. Additionally, existing guidance related to the draft biometric standard does not offer the necessary information to help agencies understand the implications of variation in the reliability and accuracy of fingerprint matching among the biometric systems being offered by vendors. Further, complete guidance for implementing FIPS 201 with regard to specific types of individuals, facilities, and information systems has not been established. Without more complete time frames and guidance, agencies may not be able to meet implementation deadlines; and more importantly, true interoperability among federal government agencies' smart card programs—one of the major goals of FIPS 201—could be jeopardized.

Recommendations

We recommend that the Director, OMB, take steps to closely monitor agency implementation progress and completion of key activities by, for example, establishing an agency reporting process, to fulfill its role of ensuring that agencies are in compliance with the goals of HSPD-12.

Further, we also recommend that the Director, OMB, amend or supplement governmentwide policy guidance regarding compliance with the FIPS 201 standard to take the following three actions:

- provide specific deadlines by which agencies implementing transitional smart card systems are to meet the "end-point" specification, thus allowing for interoperability of smart card systems across the federal government;

- provide guidance to agencies on assessing risks associated with the variation in the reliability and accuracy among biometric products, so that they can select vendors that best meet the needs of their agencies while maintaining interoperability with other agencies, and

- clarify the extent to which agencies should make risk-based assessments regarding the applicability of FIPS 201 to specific types of facilities, individuals, and information systems, such as small offices, foreign nationals, and volunteers. The updated guidance should (1) include criteria that agencies can use to determine precisely what circumstances call for risk-based assessments and (2) specify how agencies are to carry out such risk assessments.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from the Administrator of E-Government and Information Technology of OMB, the Acting Associate Administrator of GSA, and the Deputy Secretary of Commerce. Letters from these agencies are reprinted in appendixes III through V. We received technical comments from the Director of the Card Access Office for Defense and, a Special Agent at OPM, via e-mail, which we incorporated as appropriate. We also received written technical comments from the Assistant Secretary for Administration for HUD and the Assistant Secretary of Policy, Management, and Budget for Interior. Additionally, representatives from NASA and Labor indicated via e-mail that they reviewed the draft report and did not have any comments. Officials from DHS did not respond to our request for comments. Officials from GSA, Commerce, HUD, Defense, Interior, and OPM generally agreed with the content of our draft report and our recommendations and provided updated information and technical comments, which have been incorporated where appropriate.

In response to our recommendation that OMB monitor agency implementation progress and completion of key activities, OMB stated that it would continue to oversee agency implementation using their existing management and budget tools to ensure compliance. However, as agencies continue to move forward with implementing FIPS 201, we believe that in order for OMB to successfully monitor agencies' progress, it will be essential for OMB to develop a process specifically for agencies to report on their progress toward implementing the standard.

Regarding our recommendation to OMB to amend or supplement government wide policy guidance regarding compliance with the HSPD-12 standard, OMB stated that it did not think that its guidance was incomplete. Officials stated that their guidance provides the appropriate balance between the need to aggressively implement the President's deadlines, while ensuring agencies have the flexibility to implement HSPD-12, based on the level of risk their facilities and information systems present. While we agree that it is important for agencies to have flexibility in implementing the standard based on their specific circumstances, we believe that OMB has not provided agencies with adequate guidance in order for them to make well-informed, risk-based decisions about when and how to apply the standard for important categories of individuals and facilities that affect multiple agencies. For example, while multiple agencies employ foreign nationals to work at their facilities, OMB does not provide guidance on how agencies should investigate these foreign nationals prior to allowing them to access U.S. government facilities and information systems. Similarly, several agencies maintain very small facilities, yet OMB does not provide guidance on the extent to which FIPS 201 should be applied at these facilities. In addition, guidance has not been provided on assessing risks associated with the variation in the reliability and accuracy among biometric products, so that agencies can select vendors that best meet their needs while maintaining interoperability across the government.

Additionally, OMB indicated that at this time, they do not have a full understanding of whether interoperability among the transitional and end-point specifications is a concern and stated that it can not comment on our recommendation to specify the time frame for when agencies implementing transitional smart card systems are to implement the end-point specification. However, our review showed that these two specifications are not interoperable and, until all agencies implement the end-state specification the interoperability objective of HSPD-12 may not be achieved.

In commenting on our report, GSA stated that they agreed with our findings, conclusions, and recommendations. In addition, it provided us with technical comments that we incorporated as appropriate. It also suggested that in order to fully demonstrate the scope and scale of implementing HSPD-12 and FIPS 201 that we provide, as background, the current state of identity management systems across the government and industry and the impact of compliance with HSPD-12. We believe that we have adequately explained the benefits of using smart card-based ID systems and have outlined several of the significant requirements that agencies must implement as part of their new PIV systems.

In Commerce’s written comments, it stated that our report was fair and balanced. It also provided technical comments that we incorporated, where appropriate.

Additionally, OMB and Commerce noted that NIST's biometric specification had recently been revised. We have made changes to our report to reflect the revised specification.

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 the Secretaries of Homeland Security, Labor, Interior, Defense, and HUD; the Directors of OMB, OPM and NIST; the Administrators of NASA and GSA; and interested congressional committees. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Should you or your staff have any questions on 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. Other contacts and key contributors to this report are listed in appendix VI.

Sincerely yours,

Linda D Koontz

Linda D. Koontz
Director, Information Management Issues

Objectives, Scope, and Methodology

Our objectives were to determine (1) actions that selected federal agencies have taken to implement the new standard and (2) challenges that federal agencies are facing in implementing the standard.

We reviewed Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standards 201 (FIPS 201), related National Institute of Standards and Technology (NIST) special publications, Office of Management and Budget (OMB) guidance, and General Services Administration (GSA) guidance. On a nonprobability basis and using the results of the 2005 Federal Computer Security Report Card—which includes an assessment of agencies' physical security—and the results of our previous reports on federal agencies' progress in adopting smart card technology,[1] we selected six agencies that represented a range of experience in implementing smart card-based identification systems. For example, we included agencies with no prior experience implementing smart card systems as well as agencies with years of experience in implementing smart card systems. The agencies we selected were the Departments of Defense, Interior, Homeland Security (DHS), Housing and Urban Development (HUD), Labor, and the National Aeronautics and Space Administration (NASA).

To obtain information on the actions these agencies have taken and plan to take to implement the standard, we analyzed documentation such as agencies' implementation plans. We also interviewed officials from selected agencies to obtain additional information on the actions their agencies took. We reviewed the completeness and appropriateness of actions reported to us. However, we did not determine whether agencies were fully compliant with HSPD-12 and FIPS 201.

To identify challenges and barriers associated with implementing the new federal identification (ID) standard, we analyzed documentation and interviewed program officials as well as officials from GSA, NIST, the Office of Personnel Management (OPM), and OMB. In addition, we presented the preliminary challenges that we identified to agency officials to obtain their feedback and concurrence on the challenges.

We performed our work at the offices of Defense, Interior, DHS, HUD, Labor, NASA, NIST, OMB, OPM, and GSA in the Washington, D.C.,

[1] GAO-03-144 and GAO-04-948.

metropolitan area from April 2005 to December 2005, in accordance with generally accepted government auditing standards.

NIST Guidelines on Implementing FIPS 201

NIST has issued several special publications providing supplemental guidance on various aspects of the FIPS 201 standard. These special publications are summarized below.

NIST Special Publication 800-73, Interfaces for Personal Identity Verification, April 2005

SP 800-73 is a companion document to FIPS 201 that specifies the technical aspects of retrieving and using the identity credentials stored in a personal identity verification (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 also outlines two distinct approaches that agencies might take to become FIPS 201 compliant and specifies a set of requirements for each: 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 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 required to implement PIV systems that meet the end-point specification.

SP 800-73 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, such 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 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, July 2005

SP 800-79 is a companion document to FIPS 201 that describes the attributes that a PIV card issuer—an organization that issues PIV cards that comply with FIPS 201—should exhibit in order to be accredited. Agency officials need complete, accurate, and trustworthy information about their PIV credential issuers to make decisions about whether to authorize their operation. Agencies can use the guidelines in this document to certify and accredit[2] the reliability of such organizations.[3]

There are four phases (initiation, certification, accreditation, and monitoring) in the certification and accreditation processes that cover a PIV credential issuer's ability to carry out its primary responsibilities in identity proofing and registration, PIV card creation and issuance, and PIV card life-cycle management.

By following the guidelines, federal agencies should be able to accomplish the following:

- Satisfy the HSPD-12 requirement that all identity cards be issued by PIV credential issuers whose reliability have been established by an official accreditation process;
- Ensure that a PIV credential provider (1) understands the requirements in FIPS 201; (2) is reliable in providing the required services; and (3) provides credible evidence that its processes were implemented as designed and adequately documented the processes in its operations plan;
- Ensure more consistent, comparable, and repeatable assessments of the required attributes of PIV credential issuers;

[2] Certification is a formal process of assessing the attributes of a PIV credential issuer to verify that the issuer is reliable and capable of enrolling approved applicants and issuing PIV cards. Accreditation is the official management decision of a Designated Accreditation Authority to authorize the operation of a PIV credential issuer after determining that the issuer's reliability has been established through appropriate assessment and certification processes.

[3] The use of SP 800-79 for accrediting the reliability of a PIV credential issuer and accrediting the security of computer systems used by the PIV credential issuer need to follow the guidance in SP 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems*, May 2004; and SP 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

- Ensure more complete, reliable, and trusted identification of federal employees and contractors in controlling access to federal facilities and information systems; and

- Make informed decisions in the accreditation process in a timely manner and by using available resources in an efficient manner.

NIST SP 800-78, Cryptographic Algorithms and Key Sizes for PIV, April 2005

FIPS 201 specifies mechanisms for implementing cryptographic techniques[4] to authenticate cardholders, secure the information stored on a PIV card, and secure the supporting infrastructure. SP 800-78 contains the technical specifications needed to implement the encryption technology specified in the standard, including cryptographic requirements for PIV keys (e.g., algorithm and key size) and information stored on the PIV card (i.e., requiring the use of digital signatures to protect the integrity and authenticity of information stored on the card).

In addition, this document specifies acceptable algorithms and key sizes for digital signatures on PIV status information (i.e., digital signatures on the certificate revocation lists or online certificate status protocol status response messages) and card management keys, which are used to secure information stored in the PIV card. For additional information on public key infrastructure technology, see our 2001 report.[5]

[4] Cryptography is the transformation of ordinary data (commonly referred to as “plaintext”) into a code form (ciphertext) and back into plaintext using a special value known as a key and a mathematical process called an algorithm. Cryptographic techniques are used in public key infrastructure systems to generate and manage electronic “certificates,” which link an individual or entity to a given public key.

[5] GAO-01-277.

NIST SP 800-85, PIV Middleware and PIV Card Application Conformance Test Guidelines (SP 800-73 Compliance), October 2005

SP 800-85 outlines a suite of tests to validate a software developer's PIV middleware[6] and card applications to determine whether they conform to the requirements specified in SP 800-73. This special publication also includes detailed test assertions[7] 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; (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.

NIST SP 800-87, Codes for the Identification of Federal and Federally Assisted Organizations, October 2005

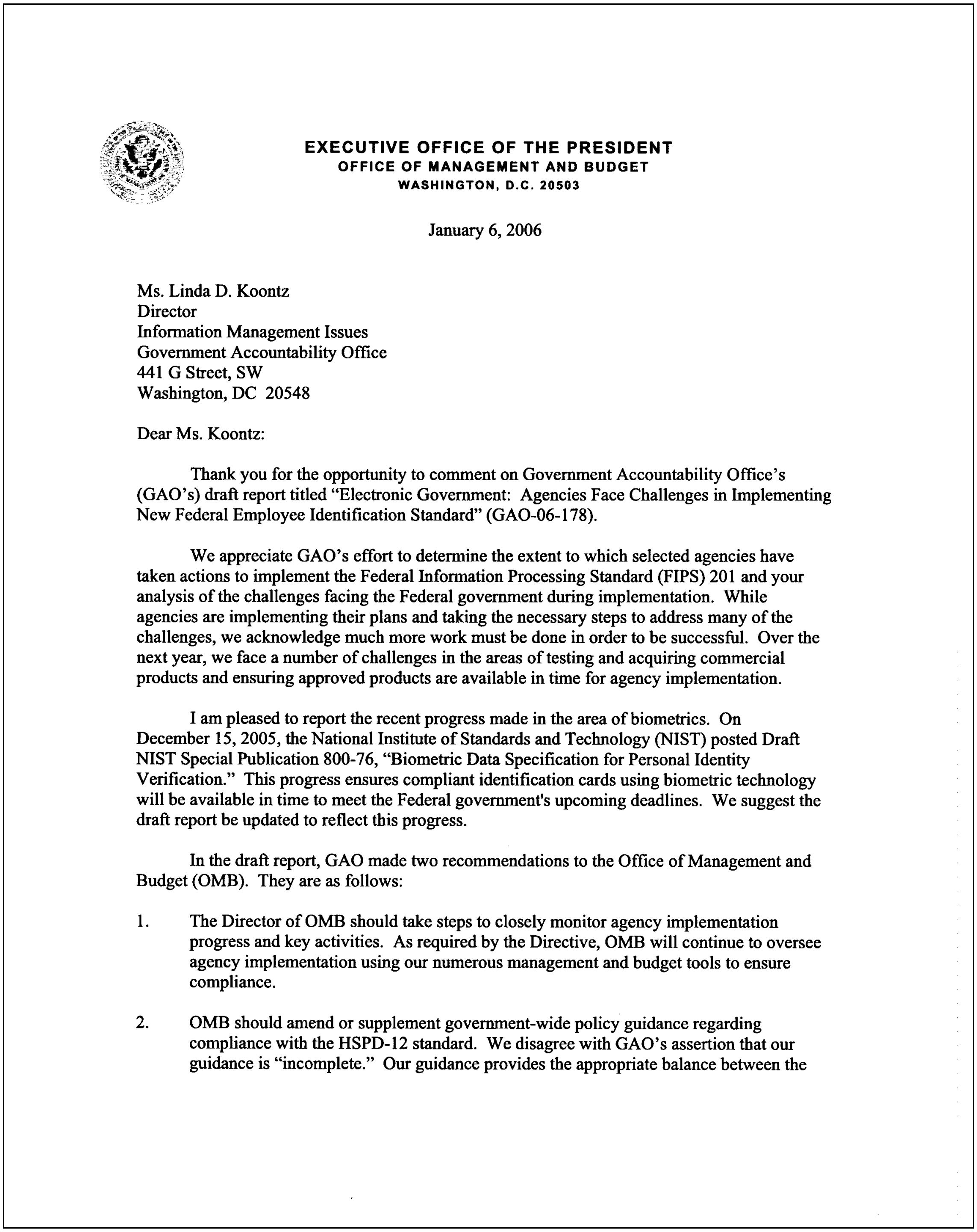
SP 800-87 outlines the organizational codes necessary to establish the unique cardholder identifier numbers.

[6] Middleware 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.

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

Appendix III

Comments from the Office of Management and Budget



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

January 6, 2006

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 Government Accountability Office's (GAO's) draft report titled "Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard" (GAO-06-178).

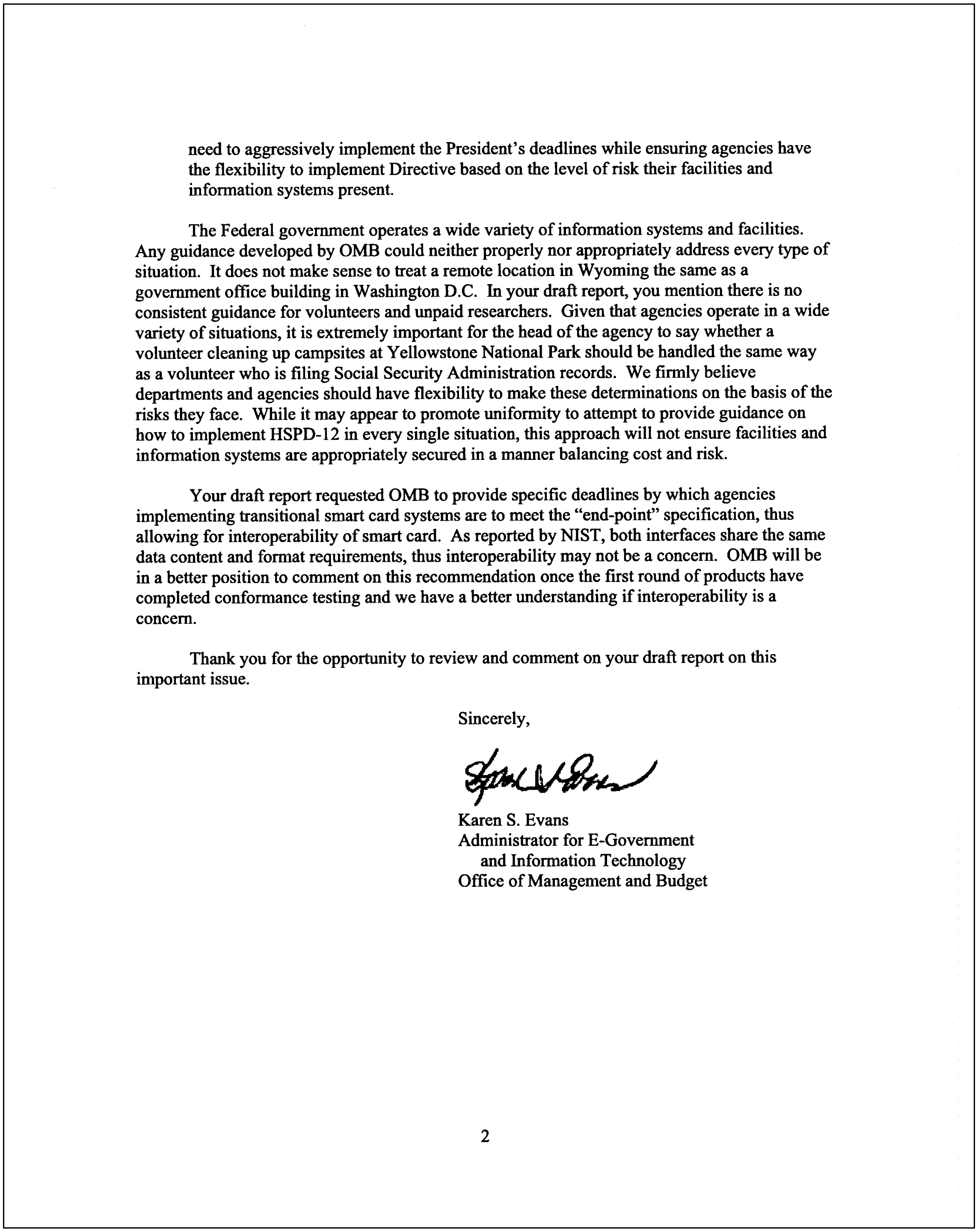
We appreciate GAO's effort to determine the extent to which selected agencies have taken actions to implement the Federal Information Processing Standard (FIPS) 201 and your analysis of the challenges facing the Federal government during implementation. While agencies are implementing their plans and taking the necessary steps to address many of the challenges, we acknowledge much more work must be done in order to be successful. Over the next year, we face a number of challenges in the areas of testing and acquiring commercial products and ensuring approved products are available in time for agency implementation.

I am pleased to report the recent progress made in the area of biometrics. On December 15, 2005, the National Institute of Standards and Technology (NIST) posted Draft NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification." This progress ensures compliant identification cards using biometric technology will be available in time to meet the Federal government's upcoming deadlines. We suggest the draft report be updated to reflect this progress.

In the draft report, GAO made two recommendations to the Office of Management and Budget (OMB). They are as follows:

1. The Director of OMB should take steps to closely monitor agency implementation progress and key activities. As required by the Directive, OMB will continue to oversee agency implementation using our numerous management and budget tools to ensure compliance.

2. OMB should amend or supplement government-wide policy guidance regarding compliance with the HSPD-12 standard. We disagree with GAO's assertion that our guidance is "incomplete." Our guidance provides the appropriate balance between the



need to aggressively implement the President's deadlines while ensuring agencies have the flexibility to implement Directive based on the level of risk their facilities and information systems present.

The Federal government operates a wide variety of information systems and facilities. Any guidance developed by OMB could neither properly nor appropriately address every type of situation. It does not make sense to treat a remote location in Wyoming the same as a government office building in Washington D.C. In your draft report, you mention there is no consistent guidance for volunteers and unpaid researchers. Given that agencies operate in a wide variety of situations, it is extremely important for the head of the agency to say whether a volunteer cleaning up campsites at Yellowstone National Park should be handled the same way as a volunteer who is filing Social Security Administration records. We firmly believe departments and agencies should have flexibility to make these determinations on the basis of the risks they face. While it may appear to promote uniformity to attempt to provide guidance on how to implement HSPD-12 in every single situation, this approach will not ensure facilities and information systems are appropriately secured in a manner balancing cost and risk.

Your draft report requested OMB to provide specific deadlines by which agencies implementing transitional smart card systems are to meet the "end-point" specification, thus allowing for interoperability of smart card. As reported by NIST, both interfaces share the same data content and format requirements, thus interoperability may not be a concern. OMB will be in a better position to comment on this recommendation once the first round of products have completed conformance testing and we have a better understanding if interoperability is a concern.

Thank you for the opportunity to review and comment on your draft report on this important issue.

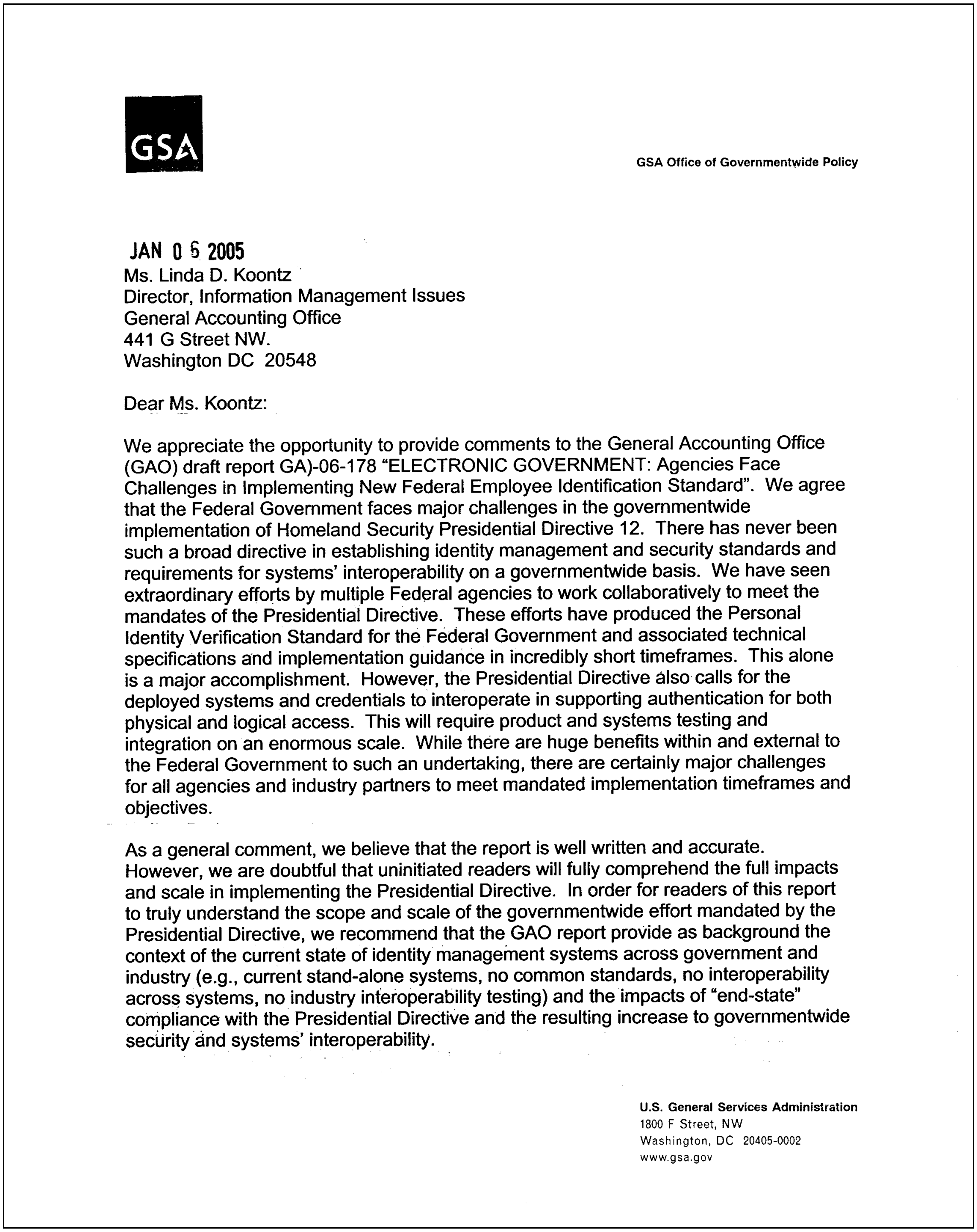
Sincerely,

Karen S. Evans
Administrator for E-Government
and Information Technology
Office of Management and Budget

2

Appendix IV

Comments from the General Services Administration



GSA Office of Governmentwide Policy

JAN 06 2005

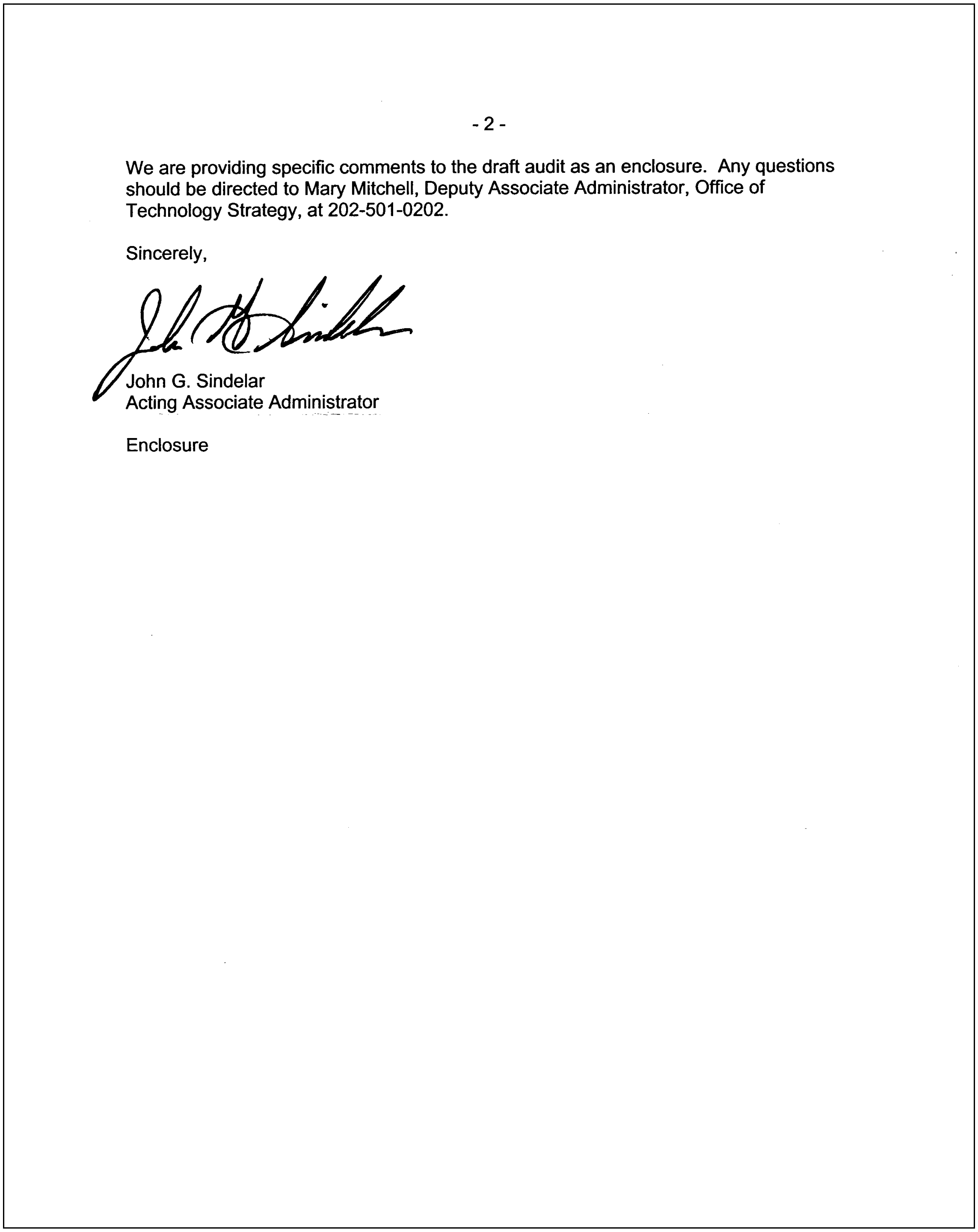
Ms. Linda D. Koontz
Director, Information Management Issues
General Accounting Office
441 G Street NW.
Washington DC 20548

Dear Ms. Koontz:

We appreciate the opportunity to provide comments to the General Accounting Office (GAO) draft report GA)-06-178 "ELECTRONIC GOVERNMENT: Agencies Face Challenges in Implementing New Federal Employee Identification Standard". We agree that the Federal Government faces major challenges in the governmentwide implementation of Homeland Security Presidential Directive 12. There has never been such a broad directive in establishing identity management and security standards and requirements for systems' interoperability on a governmentwide basis. We have seen extraordinary efforts by multiple Federal agencies to work collaboratively to meet the mandates of the Presidential Directive. These efforts have produced the Personal Identity Verification Standard for the Federal Government and associated technical specifications and implementation guidance in incredibly short timeframes. This alone is a major accomplishment. However, the Presidential Directive also calls for the deployed systems and credentials to interoperate in supporting authentication for both physical and logical access. This will require product and systems testing and integration on an enormous scale. While there are huge benefits within and external to the Federal Government to such an undertaking, there are certainly major challenges for all agencies and industry partners to meet mandated implementation timeframes and objectives.

As a general comment, we believe that the report is well written and accurate. However, we are doubtful that uninitiated readers will fully comprehend the full impacts and scale in implementing the Presidential Directive. In order for readers of this report to truly understand the scope and scale of the governmentwide effort mandated by the Presidential Directive, we recommend that the GAO report provide as background the context of the current state of identity management systems across government and industry (e.g., current stand-alone systems, no common standards, no interoperability across systems, no industry interoperability testing) and the impacts of "end-state" compliance with the Presidential Directive and the resulting increase to governmentwide security and systems' interoperability.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov



- 2 -

We are providing specific comments to the draft audit as an enclosure. Any questions should be directed to Mary Mitchell, Deputy Associate Administrator, Office of Technology Strategy, at 202-501-0202.

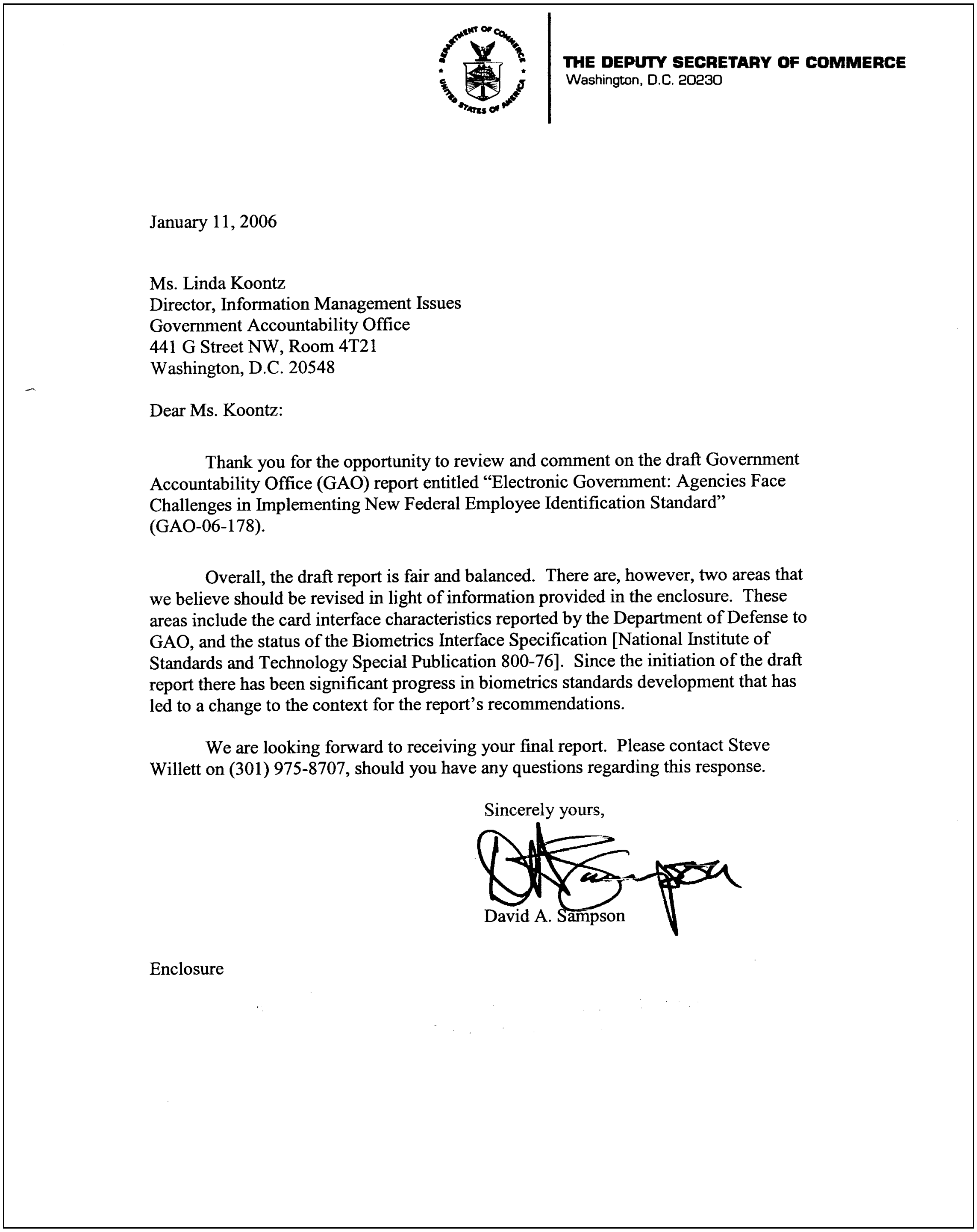
Sincerely,

John G. Sindelar
Acting Associate Administrator

Enclosure

Appendix V

Comments from the Department of Commerce



THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

January 11, 2006

Ms. Linda Koontz
Director, Information Management Issues
Government Accountability Office
441 G Street NW, Room 4T21
Washington, D.C. 20548

Dear Ms. Koontz:

Thank you for the opportunity to review and comment on the draft Government Accountability Office (GAO) report entitled "Electronic Government: Agencies Face Challenges in Implementing New Federal Employee Identification Standard" (GAO-06-178).

Overall, the draft report is fair and balanced. There are, however, two areas that we believe should be revised in light of information provided in the enclosure. These areas include the card interface characteristics reported by the Department of Defense to GAO, and the status of the Biometrics Interface Specification [National Institute of Standards and Technology Special Publication 800-76]. Since the initiation of the draft report there has been significant progress in biometrics standards development that has led to a change to the context for the report's recommendations.

We are looking forward to receiving your final report. Please contact Steve Willett on (301) 975-8707, should you have any questions regarding this response.

Sincerely yours,

David A. Sampson

Enclosure

Contacts and Staff Acknowledgments

GAO Contact

John de Ferrari, (202) 512-6335

Staff Acknowledgments

In addition to the person named above, Devin Cassidy, Derrick Dicoi, Neil Doherty, Sandra Kerr, Steven Law, Shannin O'Neill, and Amos Tevelow.

Glossary

Application programming interface

The interface between the application software and the application platform (i.e., operating system), across which all services are provided.

Authentication

The process of confirming an asserted identity with a specified or understood level of confidence.

Authorization

The granting of appropriate access privileges to authenticated users.

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.

Biometric template

A digital record of an individual's biometric features. Typically, a "livescan" 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.

Card edge

The set of command and response messages that allow card readers to communicate effectively with the chips embedded on smart cards.

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—”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 has 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.

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 recognizable.

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.

Middleware

Software that allows applications running on separate computer systems to communicate and exchange data.

Minutiae

Key data points—especially ridge bifurcations and end lines—within an individual's fingerprint that can be extracted and used to match against the same individual's live fingerprint.

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 (PIV) 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.

PIV issuer

An accredited and certified organization that procures FIPS 201 compliant blank smart cards, initializes them with 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 appropriate instructions for protection and use.

PIV 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 to ensures that a proper background check was completed before the credential and the PIV card is issued to the individual.

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 (PKI)

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, Institute of Electrical and Electronics Engineers, International Organization for Standardization, and others on a given topic—specifying the characteristics that are usually measurable, and must be satisfied in order 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 "Subscribe to 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, D.C. 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

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

PRINTED ON ♻ RECYCLED PAPER