United States Government Accountability Office

GAO

Testimony

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

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

EMPLOYEE SECURITY

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

Statement of
Linda D. Koontz
Director, Information Management Issues

Brenda S. Farrell
Director, Defense Capabilities and Management

GAO-08-551T

April 9, 2008

EMPLOYEE SECURITY

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

GAO Accountability • Integrity • Reliability

Highlights

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

Why GAO Did This Study

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

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

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

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

What GAO Found

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

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

Mr. Chairman and Members of the Subcommittee:

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

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

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

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

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

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

Results in Brief

Much work had been accomplished to lay the foundations for implementation of HSPD-12, a major governmentwide undertaking.

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

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

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

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

steps to develop guidance to help enable the exchange of identity information across agencies, and they planned to complete and issue it by September 2008.

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

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

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

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

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

Background

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

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

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

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

FIPS 201: Personal Identity Verification of Federal Employees and Contractors

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

Personal Identity Verification I

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

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

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

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

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

Personal Identity Verification II

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

Figure 1: A PIV Card Showing Major Physical Features

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

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

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

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

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

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

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

Additional NIST, OMB and GSA Guidance

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

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

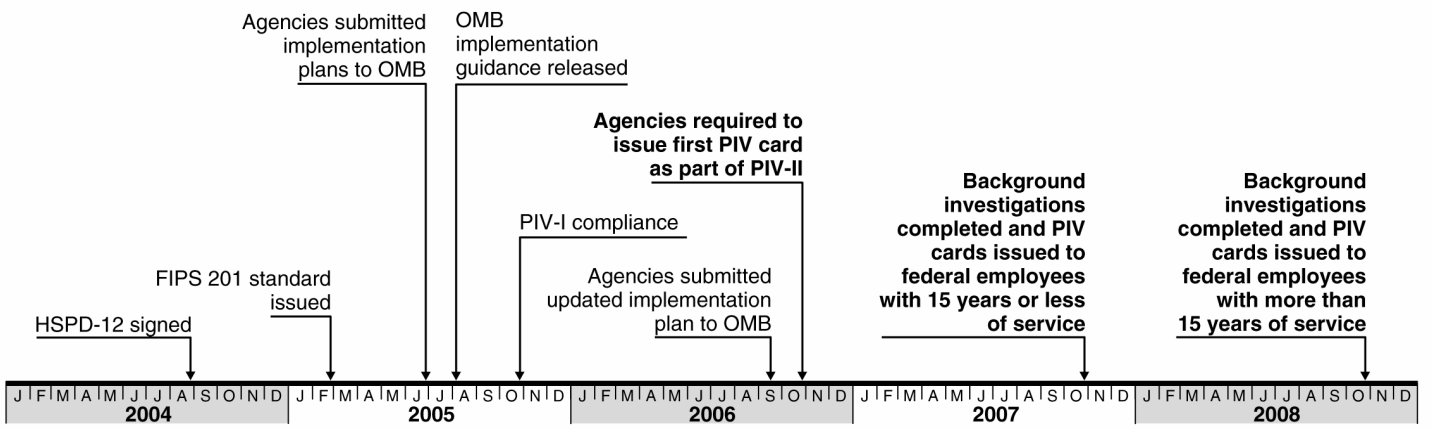
[10]For more information on NIST's guidance see GAO-08-292.

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

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

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

Figure 2: Timeline of HSPD-12-Related Activities



Source: GAO analysis of FIPS 201 guidance.

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

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

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

Previously Reported FIPS 201 Implementation Challenges

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

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

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

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

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

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

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

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

[13]5 C.F.R. § 1312.4 (2007).

[14]GAO-05-207.

[15]GAO-07-310.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Source: GAO analysis of documentation provided by agency officials.

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

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

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

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

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

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

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

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

OMB's Implementation Milestones Have Been Narrowly Focused

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[18] GAO-06-178.

[19] GAO-06-178.

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

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

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

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

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

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

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

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

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

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

Delays in Clearance Processes Continue to Be a Challenge

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

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

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

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

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

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

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

[22]GAO-08-470T.

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

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

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

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

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

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

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

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

[25]GAO-08-350.

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

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

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

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

Contacts and Acknowledgements

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

(311115)

Abbreviations

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

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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