Issue Date	
	August 28, 2007
Audit Report Number	
	2007-DP-0006

TO: Keith Nelson, Assistant Secretary for Administration, A
Bajinder Paul, Acting Chief Information Officer, Q
Joseph Neurauter, Chief Procurement Officer, N

FROM: 
Hanh Do, Director, Information Systems Audit Division, GAA

SUBJECT: Review of HUD's Personal Identity Verification and Privacy Program

HIGHLIGHTS

What We Audited and Why

We audited the U.S. Department of Housing and Urban Development's (HUD) efforts to implement the common identification standards for contractors and federal employees specified in Homeland Security Presidential Directive 12 (HSPD 12) and assessed whether those efforts complied with federal laws and guidelines governing privacy, personnel security, and information technology security. We evaluated (1) HUD's compliance with the HSPD 12 implementation schedule promulgated by the Office of Management and Budget (OMB), (2) whether controls over the issuance of personal identity verification credentials were adequate to ensure that the credentials were issued only to duly authorized and properly authenticated individuals, and (3) the adequacy of security over the systems supporting HUD's personal identity verification and privacy program.

What We Found

HUD has made progress in implementing the personal identity verification requirements of HSPD 12. However, several matters require management attention to ensure the successful implementation and long-term security of

HUD's personal identity verification and privacy program: (1) HUD did not meet all deadlines for establishing its personal identity verification process, as mandated by OMB; (2) HUD did not follow the personal identity proofing, registration, and issuance process required by OMB; and (3) HUD did not take appropriate steps to ensure adequate security over the systems supporting its personal identity verification and privacy program.

What We Recommend

We recommend that the Office of Security and Emergency Planning (1) ensure HSPD 12 requirements are fully implemented by establishing formal agreements with other HUD offices to confirm understanding of their responsibilities under the Directive; and (2) ensure that the personal identity verification process and supporting information systems, including all components, are properly certified and accredited in accordance with National Institute of Standards and Technology requirements before being placed into full-scale production.

We recommend that the Office of the Chief Information Officer ensure that (1) systems with personally identifiable information are categorized properly by program offices and (2) all HUD systems comply with backup requirements stated in National Institute of Standards and Technology Special Publication 800-53, especially systems with moderate and high impact levels.

We recommend that the Office of the Chief Procurement Officer develop a process to ensure that contracting officers include contract language to implement HSPD 12 standards for all applicable new and existing contracts.

For each recommendation without a management decision, please respond and provide status reports in accordance with HUD Handbook 2000.06, REV-3. Please furnish us copies of any correspondence or directives issued because of the audit.

Auditee's Response

The complete text of the auditees' responses, along with our evaluation of that response, can be found in the appendixes of this report.

TABLE OF CONTENTS

BACKGROUND AND OBJECTIVES

Homeland Security Presidential Directive 12 (HSPD 12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a federal standard for secure and reliable forms of identification for federal employees and contractors. The objective of HSPD 12 is to eliminate "wide variations in the quality and security of forms of identification" used to access secure federal facilities and information resources. It reiterates "the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy." To further these aims, HSPD-12 calls for establishing "a mandatory, government-wide standard for secure and reliable forms of identification." Executive departments and agencies are required to implement this standard.

The primary purpose of HSPD 12 is to direct the attention of federal government managers to the processes they use to issue and maintain their identification credentials, the methods they use to validate and attest to those processes, and the management of risk and quality throughout the life-cycle of the credential. This is consistent with major information technology and security policy initiatives for federal agencies including the Federal Information Security Management Act of 2002[1]; Office of Management and Budget (OMB) Circular A-130, appendix III[2]; and various OMB technology guidance memorandums, all of which place major emphasis on agency managers becoming more effective at managing risk, rather than relying mainly on technology adoption as the solution to information processing and security needs.

OMB provided the instructions and an aggressive implementation schedule for federal agencies to follow in implementing HSPD 12. OMB Memorandum M-05-24[3] notes that inconsistent agency approaches to facility security and computer security are inefficient and costly and increase risks to the federal government. Successful implementation of HSPD 12 will increase the security of federal facilities and information systems.

The National Institute of Standards and Technology published Federal Information Processing Standards Publication 201[4] to satisfy the technical and administrative requirements and meet the ambitious deadlines established by HSPD 12 and OMB. Part one of the standard describes the minimum requirements for a federal personal identification system that meets the control and security objectives of HSPD 12, including the personal identity proofing, registration, and issuance process that was to have been in place beginning October 27, 2005. The second part of the standard specifies the implementation, technical, and interoperability requirements of the personal identity verification system that was to have been in place beginning October 27, 2006. Also, HSPD 12 and the standard require agencies to protect personal privacy information when implementing their personal identity verification systems.

[1] Public Law 107-347, Title III.
[2] Security of Federal Automated Information Resources.
[3] "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," dated August 5, 2005.
[4] Personal Identity Verification (PIV) of Federal Employees and Contractors, dated March 2006.

Within the U.S. Department of Housing and Urban Development (HUD), the Office of Security and Emergency Planning has overall responsibility for HUD's personal identity verification program and implementation of all aspects of HSPD 12. This responsibility includes serving as the main internal and external point of contact with respect to program planning, operations, business management, communications, and technical strategy. The Office of the Chief Information Officer provides the infrastructure and logical access for the operation of the personal identity verification systems. The Office of the Chief Procurement Officer is responsible for ensuring that new and existing contracts extend the personal identity verification requirements of HSPD 12 to contractors who require long-term access to HUD's facilities and systems.

HUD has made progress in implementing the personal identity verification requirements of HSPD 12. For instance,

- HUD developed and published guidance in support of HSPD 12 and OMB's implementation instructions.
- HUD performed privacy impact assessments for the two new systems, Identity Management System and Card Management System, that will support HUD's personal identity verification process.
- In addition to providing training and certification to more than 100 employees at headquarters and field offices as personal identity verification registrars, the Office of Security and Emergency Planning provided briefings to employees, such as administrative officers, human resource specialists, government technical representatives, and government technical monitors, on HSPD 12 and the new personal identity verification process.
- HUD established a Web site to keep employees abreast of HSPD 12-related developments.
- HUD has nearly completed the installation of its HSPD 12-compliant card readers that grant physical access to its headquarters building in Washington, DC. Published reports indicate that most government agencies will require three to five years to upgrade their access control systems in support of HSPD 12.

The objective of our audit was to evaluate HUD's efforts to implement a personal identity verification and privacy program in accordance with federal security and privacy laws and policies. To accomplish this, we evaluated (1) HUD's compliance with the HSPD 12 implementation schedule promulgated by OMB, (2) whether controls over the issuance of personal identity verification credentials were adequate to ensure that the credentials were issued only to duly authorized and properly authenticated individuals, and (3) the adequacy of security over the systems supporting HUD's personal identity verification and privacy program.

We conducted this audit as a component of our annual consolidated financial statements audit and our annual evaluation of HUD's information system security program required by the Federal Information Security Management Act of 2002.

RESULTS OF AUDIT

Finding 1: HUD's Personal Identity Verification Process Does Not Fully Comply with OMB and NIST Requirements

HUD's personal identity verification process was not fully implemented as required by OMB Memorandum M-05-24 and National Institute of Standards and Technology Federal Information Processing Standards Publication 201. Specifically, (1) deficiencies were identified in HUD's personal identity proofing, registration, and issuance process; and (2) HUD did not meet all deadlines specified by OMB for the implementation of its personal identity verification process. A lack of formalized agreements between offices that provide HSPD 12-related services, as well as time and resource constraints, prevented HUD from adequately monitoring its personal identity verification process. Additionally, HUD's current personal identity verification systems and the automated systems that support HUD's procurement activities lack the ability to generate reports with useful information to assist officials in meeting the deadlines specified by OMB. These lapses undermine efforts to improve the overall security of federal information resources and facilities.

The personal identity verification process encompasses procedures designed to ensure that only qualified individuals are granted access to federal facilities and information systems. The process includes specific steps for verifying the true identity of each individual and performing background investigations to determine their suitability for employment. Every federal agency must implement these steps to meet HSPD 12's objective of eliminating the "wide variations in the quality and security of forms of identification" used to access secure federal facilities and information resources.

To underscore the importance of HSPD 12, the president established an aggressive timeframe for implementing its requirements. Once the standard for secure and reliable forms of identification was promulgated, agencies were given four months to establish a program to ensure that identification issued to federal employees and contractors met the standard. Additionally, within eight months of the promulgation of the standard, agencies were to require that employees and contractors use the identification credentials to gain physical access to federally controlled facilities and logical access to federally controlled information systems. OMB Memorandum M-05-24 provided the specific deadlines and instructions for implementing the requirements of HSPD 12.

Another goal of HSPD 12 is to provide identity credentials that can be trusted and acceptable to all federal agencies. To foster this trust and acceptability, each agency's personal identity verification process and supporting information systems must be certified and accredited. The certification must be performed by an individual who is independent of the office responsible for issuing identification cards and correcting deficiencies and discrepancies identified during the certification phase. The independence of the certification agent is an important factor in assessing the credibility of the assessment results.

Continual monitoring of the personal identity verification process is required to identify changes that may impact the reliability of the personal identity verification system or any of its components. Within HUD, responsibility for monitoring the personal identity verification process was assigned to the independent certification agent.

HUD Did Not Consistently Follow All Personal Identity Verification Procedures and Policies

The Office of Security and Emergency Planning did not ensure that identification cards were issued in accordance with published personal identity verification requirements.

The automated systems that support HUD's current personal identity verification process have limited reporting capabilities. HUD's personal identity verification files are, for the most part, paper based. As a result, HUD was unable to provide the universe of employees, contractors, or identification badges issued since the new personal identity verification process was put into place.

We manually selected a random sample of 47 (23 employees and 24 contractors) paper-based personal identity verification files maintained for HUD employees and contractors for evaluation. Six of the files were for identification badges issued before October 27, 2005, and eight files contained cancelled requests because access was not needed. We excluded these 14 files from our analysis. The remaining 33 files were for identification badges issued to employees and contractors after October 27, 2005, the deadline established by OMB to begin following the personal identity proofing, registration, and issuance guidelines promulgated in Federal Information Processing Standards Publication 201.

- Of the 33 personal identity verification files reviewed, we identified 20 instances (12 new contractors and 8 new employees) in which identification badges were issued before the completion of the Federal Bureau of Investigation National Criminal History Check (fingerprint check).
- We also identified 18 instances (11 contractors and 7 employees) in which identification badges were issued before the National Agency Check with Written Inquiries (background investigation) was initiated. For example, the background investigation for one contractor was not initiated until five months after the contractor received an identification badge.

- Identification badges were issued to 8 of 24 new contractors and employees without proper forms of identification. For instance, an identification badge was issued to a new employee who provided two documents that established identity but none that established employment eligibility.

Additionally, the Office of Security and Emergency Planning did not revoke the identification badges of new employees and contractors whose background investigations were not completed within six months. Badges were often issued based solely on a successful fingerprint check. In some instances, employees and contractors had the identification badges to access HUD's facilities for more than a year before full background investigations were completed.

HUD Did Not Monitor Its Personal Identity Verification Process

HUD did not monitor its personal identity verification process to ensure that published procedures and policies were being followed. Initially, the responsibility for monitoring was assigned to the independent certification agent, an employee of the Office of the Chief Information Office. However, the employee accepted a position within the Office of Security and Emergency Planning, which has overall responsibility for HUD's personal identity verification program. As a result, the employee became ineligible to perform the duties of an independent certification agent and duties assigned in conjunction with the new position further precluded monitoring of HUD's personal identity verification process.

Officials from the Office of Security and Emergency Planning assumed that since the Office of the Chief Information Officer initially provided the certification agent, it would continue to provide this service. However, there was no formal agreement between the offices for this service, and responsibility for certifying and monitoring the personal identity verification process was never documented or formally established. HUD has yet to reassign the responsibilities for continual monitoring of the personal identity verification process.

Had monitoring been performed, the irregularities identified in the preceding section could have been identified and corrected sooner. HUD is now in the process of reviewing and verifying information in its paper-based personal identity verification files for each identification card issued at headquarters to ensure that the process has been properly implemented.

HUD's Contracting Officers Did Not Always Include Contract Language to Implement the Personal Identity Verification Requirements of HSPD 12

HUD's contracting officers did not always include contract language to implement the personal identity verification requirements of HSPD 12 in new contracts (including options being exercised) by October 2005 as required by OMB.

The current automated systems used by contracting officers to manage contracts cannot identify the universe of contracts in which the contractors require access to HUD facilities and/or systems. As a result, the Office of the Chief Procurement Officer cannot monitor to ensure that contracting officers include HSPD 12 requirements in applicable existing contracts when contract options are exercised.

- From a list of all contract actions identified as having options exercised between October 27, 2005, and January 31, 2007, we randomly selected 18 contracts. Of the 18 contracts reviewed, five required contractor personnel to have facility and/or system access. In four of the five contracts, modifications to incorporate the personal identity verification clause were not issued at the time the options were exercised. Modifications to add the personal identity verification clause were later generated and approved for two contracts, and two other personal identity verification modifications are currently awaiting management approval.

- From a list of all new contracts awarded between October 27, 2005, and January 31, 2007, we randomly selected 14 contracts. Eleven of the contracts required contractor personnel to have facility and/or system access. One of the contracts contained an outdated personnel security clause, which was crafted more than two years before the HSPD 12 legislation.

Conclusion

HUD did not follow published guidelines for the personal identity verification process promulgated by HSPD 12. It also did not meet all deadlines specified by OMB for the implementation of part two of the personal identity verification standard of HSPD 12. A lack of formalized agreements between offices that provide HSPD 12-related services, as well as time and resource constraints, prevented HUD from adequately monitoring its personal identity verification

process. Additionally, HUD's current personal identity verification systems and the automated systems that support HUD's procurement activities lack the ability to generate reports with useful information to assist officials in meeting the deadlines specified by OMB. By not following federal requirements for securely granting access to HUD's facilities and information systems, HUD is at increased risk that unauthorized, ineligible individuals may be granted access to sensitive information and facilities. Additionally, these lapses undermine efforts to improve the overall security of federal information and facilities and call into question the credibility of HUD's personal identity verification process.

Recommendations

We recommend that the Office of Security and Emergency Planning

1A. Document the HSPD 12-related roles and responsibilities of other HUD offices and establish formal agreements to confirm understanding of these responsibilities.

1B. Ensure that personal identity verification registrars, issuers, and adjudicators fully understand the requirements for identity proofing and credential issuance.

1C. Revise HUD's personal identity verification guidance to

- Clearly reflect all federal personal identity verification requirements, including the need to complete the Federal Bureau of Investigation fingerprint check (i.e., receive the results of the fingerprint check).
- Update and/or remove policies no longer in practice, such as revoking building and system access if background investigations are not completed within six months. If the six-month revocation requirement is removed, ensure that a suitable process is put in place to ensure that access is revoked if background investigations are not completed within a reasonable timeframe.
- Define the roles and responsibilities of other HUD offices as they relate to the personal identity verification program.

1D. Establish a process for the continual monitoring of HUD's personal identity verification process.

We recommend that the Office of the Chief Procurement Officer

1E. Develop a process to ensure that contracting officers include contract language to implement HSPD 12 standards for all applicable new and existing contracts.

1F. Develop a mechanism to readily identify contracts in which access to federally controlled facilities and/or information systems will be required.

Finding 2: HUD Did Not Take Appropriate Steps to Ensure Adequate Security over the Systems Supporting Its Personal Identity Verification and Privacy Program

HUD did not ensure that the systems supporting its personal identity verification and privacy program complied with federal information security requirements. We determined that (1) new systems were placed into production before full certification testing was completed; (2) the systems currently supporting HUD's personal identity verification process were not certified and accredited and did not follow federal guidelines for the backup of sensitive, personally identifiable information; (3) the initial certification and accreditation of HUD's personal identity verification process was incomplete and expired in April 2007; and (4) HUD has 14 systems with security categorizations rated as low impact that contain personally identifiable information. These conditions occurred because personnel responsible for HUD's personal identity verification and privacy program were not aware of all information security requirements and did not fully understand their security responsibilities. As a result, HUD cannot be assured that its systems will operate as intended and are protected from unauthorized access, use, modification, or destruction. Thus, the confidentiality, availability, and integrity of sensitive information entrusted to HUD could be at risk.

Security certification and accreditation are important activities that support a risk management process and are an integral part of an agency's information security program. Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. To effectively manage information security, agencies must maintain an inventory of major systems.

The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

The information technology system(s) used by personal identity verification service providers must be certified to fully accomplish the accreditation of personal identity verification service

providers. Identity credentials can only be issued through systems and providers, the reliability of which has been established by the agency and so documented and approved in writing (i.e., accredited).

System data should be backed up regularly. Agency policies should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality and the frequency with which new information is introduced. At minimum, systems containing personally identifiable information should fall into the moderate impact security category. It is good business practice to store backed up data off site in a secure, environmentally controlled facility. If users back up data on a stand-alone system rather than saving data to the network, a means should be provided for storing the media at an alternate site.

HUD Placed a New System Into Production Before Full Certification Testing Was Completed

HUD's new Identity Management System,[5] which is currently in pilot phase, is being used in HUD's personal identity verification process to issue new identification badges and in preparation for the issuance of new identity credentials to headquarters employees. However, neither the system in its entirety nor its individual components have been certified or accredited. For instance, the Office of Security and Emergency Planning placed a new, automated fingerprint system (Cross Match 700) into production without certifying and accrediting the system. This system is now included as a component of the new Identity Management System, which has not been fully tested.

HUD began processing employees and contractors using the new Identity Management System on June 11, 2007. The Office of the Chief Information Officer awarded a contract to perform certification and accreditation on the new Identity Management System and HUD's personal identity verification process in May 2007, but the work is still ongoing.

[5] The Identity Management System is a computer application and database used during the personal identity verification registration process. It creates the applicant's enrollment record and manages and maintains this information throughout the personal identity verification card lifecycle. The Identity Management System is also used to verify, authenticate, and revoke cardholder access to federal facilities (buildings and office space). Likewise, the Identity Management System is the key data source for verifying identity when cardholders seek "logical" access to federal information systems (using the electronic authentication features of the combination ID badge/smart card).

The Systems Currently Supporting HUD's Personal Identity Verification Process Were Neither Certified nor Accredited

The Office of Security and Emergency Planning did not certify and accredit the systems that currently support its personal identity verification process (DSX card management system and Security Control and Access Tracking System). The systems have been in production for several years without certification and accreditation or supporting security documentation. Additionally, the DSX card management system, which controls physical access to HUD's headquarters, is not included in HUD's inventory of automated systems.

HUD's Information Technology Security Policy Handbook notes that program offices and system owners are responsible for the certification and accreditation of their systems. However, the Office of Security and Emergency Planning did not take steps to provide security certifications for these systems. Officials from the Office of Security and Emergency Planning incorrectly believed that since the Office of the Chief Information Officer did not support the current systems, certification and accreditation were not required. Furthermore, the officials did not believe that they needed to report the DSX card management system to the Office of the Chief Information Officer for inclusion in the inventory of automated systems because it is a small system (contains a small database) and purportedly is not supported by the chief information officer.

Information Systems Currently Supporting HUD's Personal Identity Verification Process Were Not Backed Up in Accordance with Federal Requirements for Systems Containing Personally Identifiable Information

HUD did not follow federal requirements for backing up the sensitive, personally identifiable information contained in the systems currently supporting is personal identity verification process. Data contained in the Security Control and Access Tracking System were not backed up. A process is in place to back up the data from the DSX card management system; however, the backup process has not been consistent. Further, backups for the DSX card management system have not been tested and are not stored in a geographically separate location from the primary processing site. Both systems contain personally identifiable information.

Officials from the Office of Security and Emergency Planning stated that they had not attended specialized training related to information security requirements and were unsure of the reason why backups for the DSX card management system were inconsistently performed. However, they believed that data in the Security Control and Access Tracking System were backed up by the Office of the Chief Information Officer through the HUD information technology services contract since it is connected to HUD's network.

The Initial Certification and Accreditation of HUD's Personal Identity Verification Process Was Incomplete and Expired in April 2007

Although HUD's personal identity verification process was certified by the Office of the Chief Information Officer and accredited by the assistant secretary for administration, the certification and accreditation are incomplete because the systems that support the personal identity verification process were not certified and accredited. Further, the certification and accreditation of HUD's personal identity verification process expired in April 2007.

The Office of Security and Emergency Planning was not aware of the requirement to certify and accredit the personal identity verification system in conjunction with the personal identity verification process. The Office of the Chief Information Officer has since awarded a contract to perform certification and accreditation on both the new Identity Management System and HUD's personal identity verification process.

The Security Impact Level of 14 Systems Containing Personally Identifiable Information Was Understated

HUD has 14 systems with security categorizations rated as low impact that contain personally identifiable information. HUD's information technology security policy does not provide specific instructions to program offices to categorize systems containing personally identifiable information as moderate impact.

Conclusion

HUD did not ensure that the systems supporting its personal identity verification and privacy program were properly certified and accredited; followed federal guidelines for backup of sensitive, personally identifiable information; and carried the appropriate security impact categorizations. The personnel responsible for HUD's personal identity verification and privacy program were not aware of all information security requirements and did not fully understand their security responsibilities. As a result, HUD cannot be assured that its systems will operate as intended and are protected from unauthorized access, use, modification, or destruction. Thus, the confidentiality, availability, and integrity of sensitive information entrusted to HUD could be at risk.

Recommendations

We recommend that the Office of Security and Emergency Planning

2A. Ensure that HUD's personal identity verification process and new Identity Management System, including all components, are fully documented, tested, certified, and accredited before being placed into full-scale production.

2B. Ensure that system owners fully understand their security responsibilities, including the categorization of systems containing personally identifiable information; inclusion of all computing resources in the departmental information system inventory; and the requirement to certify, accredit, and provide security documentation for all systems.

2C. Ensure that the systems currently supporting HUD's personal identity verification system are backed up and that the backups are tested before the information is imported into the new Identity Management System.

We recommend that the Office of the Chief Information Officer

2D. Ensure that information system owners receive information security training to ensure compliance with federal and HUD-issued information security requirements.

2E. Ensure that system owners comply with federal and HUD-issued requirements to back up systems and data, particularly those systems with moderate and high security impact levels.

2F. Update its Information Technology Security Policy Handbook to specify that systems with personally identifiable information should be categorized as moderate or high impact.

2G. Notify system owners identified as having systems with security categorizations rated as low impact that contain personally identifiable information and instruct them to update the security categorizations.

SCOPE AND METHODOLOGY

We performed the audit

- From January through June 2007,
- At HUD headquarters, Washington, DC, and
- In accordance with generally accepted government auditing standards.

Our assessment focused on reviewing actions taken by HUD to implement the personal identity verification requirements of HSPD 12 and evaluating the security controls in place for systems with personally identifiable information.

We performed a detailed review of HUD's personal identity verification process based on guidelines contained in memorandums from OMB and federal information processing standards and special publications by the National Institute of Standards and Technology.

HUD's personal identity verification files are, for the most part, paper based. The automated systems that support HUD's current personal identity verification process have limited reporting capabilities. As a result, we were unable to obtain the universe of employees, contractors, or identification badges issued since the new personal identity verification process was put into place. Consequently, we manually selected for review a sample of paper-based personal identity verification files maintained for HUD employees and contractors. We selected personal identity verification documents for the first employee or contractor in each paper folder. This process yielded 47 (23 employees and 24 contractors) personal identity files for evaluation. Thirty-three of the selected files were for identification badges issued to employees and contractors after October 27, 2005.

We used a random statistical sampling method to determine whether HUD's Office of the Chief Procurement Officer included contract language to implement the requirements of HSPD 12 in new contracts (including contract options being exercised) that provide contractors access to HUD's facilities and systems by the October 2005 implementation deadline established by OMB.

The automated systems used by the Office of the Chief Procurement Officer are not able to identify contracts that require contractors to have long-term access to HUD-controlled facilities or information systems. Instead, the office provided us with the following listings: (1) a list of all new contracts awarded between October 27, 2005, and January 31, 2007, and (2) a list of all contract actions identified as having options exercised between October 27, 2005, and January 31, 2007.

- From the list of new contracts, we limited our population to only those new contracts awarded at HUD headquarters in Washington, DC. From this limited population, 14 contracts were selected for review. The 14 contracts included all contracts awarded in

calendar years 2005 (three contracts) and 2007 (one contract) and 10 randomly selected contracts awarded in calendar year 2006. The 10 randomly selected contracts were selected using statistical sampling software. Of the 14 new contracts available for review, 11 required contractors to have access to HUD's facilities and/or information systems.

- For the list of contract options that were exercised, we randomly selected 18 contracts (six contracts each from years 2005, 2006, and 2007) using statistical sampling software. Of the 18 contracts selected for review, only five required contractors to have access to HUD's facilities and/or information systems.

To accomplish our objectives, we obtained and analyzed information supporting HUD's efforts to implement the common identification standards for contractors and federal employees specified in HSPD 12. In addition, we obtained and reviewed federal requirements and guidelines, including memorandums issued by OMB and special publications and federal information processing standards publications issued by the National Institute of Standards and Technology. We also reviewed HUD management reports and conducted interviews with key personnel in the Office of Security and Emergency Planning, Office of the Chief Information Officer, and Office of the Chief Procurement Officer.

INTERNAL CONTROLS

Internal control is an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved:

- Effectiveness and efficiency of operations,
- Reliability of financial reporting, and
- Compliance with applicable laws and regulations.

Internal controls relate to management's plans, methods, and procedures used to meet its mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance.

Relevant Internal Controls

We determined the following internal controls were relevant to our audit objectives:

- Policies, procedures, management, and operational and technical controls used for implementing an effective personal identity verification and credential issuance process that are compliant with the requirements of HSPD 12.
- Policies, procedures, management, and operational and technical controls used for protecting personal identity verification systems and systems with personally identifiable information.

We assessed the relevant controls identified above.

A significant weakness exists if management controls do not provide reasonable assurance that the process for planning, organizing, directing, and controlling program operations will meet the organization's objectives.

Significant Weaknesses

Based on our review, we believe the following items are significant weaknesses:

- HUD identification cards were issued before Federal Bureau of Investigation fingerprint checks were completed and/or before background investigations were initiated. Access to HUD's facilities and information systems was not revoked when background investigations were not completed within a reasonable timeframe (finding 1).
- The Office of Security and Emergency Planning did not document all roles and responsibilities associated with HUD's personal identity verification

program and did not establish formal agreements with other HUD offices that provide HSPD 12-related services to confirm understanding and acceptance of the responsibilities (finding 1).

- HUD issued identification cards and credentials using information systems that have not been certified and accredited (finding 2).

Appendix A

OSEP's COMMENTS AND OIG'S EVALUATION

Comment 1

Comment 2

OFFICE OF ADMINISTRATION'S COMMENTS TO DRAFT AUDIT REPORT – Review of HUD's Personal Identity Verification and Privacy Program

No	Reference	Audit Report Statement	ADMIN Comment
1	Page 1, "What We Found", 1st paragraph, #(1)	"HUD did not meet all deadlines for establishing its personal identity verification process, as mandated by OMB, and will not meet all remaining implementation deadlines..."	HUD did meet the major OMB milestones regarding HSPD-12 and OMB's memorandum M-05-24 concerning the implementation of FIPS-201 PART 1: PIV-I. Due to budget constraints, the availability of HSPD-12 compliant products, and other factors beyond our control, HUD acknowledges that it has not yet fully implemented FIPS-201 PART 2: PIV-II but does not feel it is justified for the OIG to state that HUD "will not meet all remaining implementation deadlines". To further ensure HUD would meet all OBM deadlines, the HUD/OSEP signed an MOU and provided funding to GSA to enroll in the GSA Shared Service Provider (SSP) program. This MOU provided HUD with the option to use GSA's PIVII SSP in the event HUD could not begin PIVII processing by the OMB due date. Unfortunately GSA was only able to provide four (4) PIVII credentials to HUD employees before their SSP program was terminated due to contract issues. The GSA SSP program has as of this date not been reactivated. HUD is still by far one of very few agencies leading the federal government's implementation and rollout of HSPD-12.
2	Page 2, "What We Found", 1st paragraph,#(2)	"HUD did not follow the personal identity proofing, registration, and issuance process required by OMB..."	HUD published the Personal Identity Verification (PIV-I), Part 1 for Federal Employees and Contractors guidance that describes the identity proofing, registration, and issuance process required by OMB. In addition, HUD conducted training for Headquarters and Field Office staff in the PIV-1 process. PIVI was a "role based" process. HUD staff adhered to the PIVI process as

Page 1

Comment 3

No	Reference	Audit Report Statement	ADMIN Comment
			much as possible but because PIVI is a "roles based" process, human error is possible. HUD is now processing employees and contractors using the PIVII process, which is a "system based" process. The "system based" process adheres to and enforces the PIVII requirements, greatly reducing the chance for human error.
3	Page 2, "What We Found", 1st paragraph,#(3)	"HUD did not take appropriate steps to ensure adequate security over systems supporting its personal identity verification and privacy program."	There is essentially one system, Security Control and Access Tracking System (SCATS) used to support the PIV-I program. SCATS is a Microsoft Access database used to support the Personnel Security Branch background investigation business process. SCATS is not FIPS-201 compliant and was only used to support the PIVI process. This particular system was initially created in the OIG Personnel Security office then moved to OHR and finally inherited by the Personnel Security Branch in OSEP. This legacy database is password protected and resides on a HUD standard network drive shared only by OSEP personnel authorized to access the data. The data is backed up by the OCIO/HITS data backup procedures. The WinDSX Access Control System (DSX) was not used to support the PIV-I process. The DSX system does not create nor support PIV credentials. DSX is another legacy system inherited from the OAMS and is used solely to manage the HUD ID badges issued to employees and contractors requiring access to HUD facilities. DSX is not FIPS-201 compliant and does not serve in the FIPS-201 PIV program. This system should not be evaluated in this audit report. In any case both SCATS and DSX are being replaced by the SecurityManager Identity Management System (IDMS).

Page 2

No	Reference	Audit Report Statement	ADMIN Comment
			The IDMS is in the process of being fully accredited and certified in accordance with the National Institute of Standards and Technology (NIST) requirements and will follow all OCIO software release procedures before being placed into production.
4	Page 2, "What We Recommend" 1st paragraph, #(1)	"Ensure HSPD-12 requirements are fully implemented by establishing formal agreements with other HUD offices..."	The HSPD-12 program is a Departmental initiative. Personnel security policies and directives related to HSPD-12 and FIPS-201 have been disseminated to all HUD employees via memorandums from the Secretary and his immediate staff. Program office Administrative Officers and OHR personnel have been trained by OSEP on the FIPS-201 PIVI process. If and where necessary OSEP will document specific and/or unique roles and responsibilities concerning other program offices in memorandums of understanding to program office managers.
5	Page 2, "What We Recommend" 1st paragraph, #(2)	"Ensure that the personal identity verification process and supporting systems, including all components, are properly certified and accredited..."	See item #3 above.
6	Page 5, 1st paragraph, 1st sentence	"Within the U.S. Department of Housing and Urban Development (HUD), the Office of Security and Emergency Planning has overall responsibility for HUD's personal identity verification program and implementation of all aspects of HSPD-12."	The OSEP is responsible for the PIVI and PIVII process as far as the issuance of PIVII credentials to HUD employees and contractors. The logical access portion of HSPD-12 is the responsibility of the Office of Information Technology (OIT) in the OCIO. OSEP and OIT are working closely together to ensure complete and successful implementation of all aspects of the HSPD-12 program.
7	Page 7, "HUD Did Not Consistently Follow All Personal Identity Verification Procedures	"The Office of Security and Emergency Planning did not ensure that identification cards were issued in accordance with published personal identity verification	See item #2 above and item #9 below.

Page 3

Comment 4

Comment 5

Comment 6

Comment 7

Comment 8

Comment 9

No	Reference	Audit Report Statement	ADMIN Comment
	and Policies", 1st paragraph	requirements."	
8	Page 7, "HUD Did Not Consistently Follow All Personal Identity Verification Procedures and Policies", 2nd paragraph,3rd sentence	"As a result, HUD was unable to provide the universe of employees, contractors, or identification badges..."	The criteria to provide the information to the OIG was available at the time of the request, but because PIVI was a paper based process, the OSEP did not have the time nor the resources available to compile the data.
9	Page 7, "HUD Did Not Consistently Follow All Personal Identity Verification Procedures and Policies", 3rd paragraph, 1st bullet	"Of the 33 personal identity verification files reviewed, we identified 20 instances...in which identification badges were issued before the completion..."	This entire section of the audit report refers to the issuance of identification cards (first paragraph of this section) or identification badges (third paragraph of this section) prior to the completion of a step in PIVI process. OSEP would like this entire section removed from the audit report. FIPS-201 and OMB memorandum M-05-24 (M5-24) specifically address processes and requirements as they relate to the issuance of PIV credentials. Memorandum M-05-24, page 5, bullet A, states: "Adopt and accredit a registration process consistent with the identity proofing, registration, and accreditation requirements in section 2.2 of the Standard and forthcoming technical guidance issued by NIST, regardless of whether your agency will be ready to issue standard compliant credentials by October 27, 2005. This registration process will apply to all new identity credentials issued (i.e. no new identity credentials can be issued until these conditions are met)." FIPS-201, Appendix F – Glossary of Terms, Acronyms, and Notations, page 70, section F.1, defines a credential as: "Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally,

Page 4

Comment 10

No	Reference	Audit Report Statement	ADMIN Comment
			additional attributes) to that individual. The identification cards and/or badges the audit report continues to reference are not FIPS-201 PIV credentials. The OSEP complied with the requirements of HSPD-12 and FIPS-201 by implementing the PIVI personal identity proofing, registration, and verification process on October 27, 2005. All new HUD employees and contractors were processed under the PIVI requirements. All current employees and contractors are now being processed under the PIVII requirements. The OSEP did not issue any PIV credentials during the audit report period.
10	Page 8, "HUD Did Not Monitor Its Personal Identity Verification Process", 3rd paragraph, 1st sentence	"Had monitoring been performed, the irregularities identified in the preceding section could have been identified and corrected sooner."	Although the OIG is correct in its assessment that the OCIO employee assigned as the independent certification agent was eventually transferred to the OSEP and therefore could no longer serve in that capacity, the statement in the first paragraph of this section "HUD did not monitor its personal identity verification process..." is not accurate. The entire PIVI program was consistently monitored by several staff members in the OSEP. Unfortunately, the PIVI process was a "roles based" paper process and the OSEP was processing hundreds of employees and contractors a month. Regular reviews of the PIVI paperwork were conducted weekly by randomly selecting enrollment documents and checking them for accuracy and compliance to the PIVI requirements. In some cases applicants were contacted to revisit the PIVI enrollment office to correct and/or verify discrepancies in their paperwork. As explained in item #2 above, PIVI is a "roles based" paper process and human error is possible. Staffing resource issues and the large

No	Reference	Audit Report Statement	ADMIN Comment
			number of employees and contractors enrolled by the paper process, made it very difficult to review each enrollment record.
11	Page 9, "HUD's Strategy to Complete Background Investigations...", 1st paragraph	"The strategy developed by the Office of Security and Emergency Planning to complete investigations...does not include either contractors or individuals who require and updated or upgraded..."	The OSEP has had a strategy in place prior to October 2005 to ensure that all HUD employees and contractors have at a minimum a National Agency Check with Written Inquires (NACI) investigation on file. The OSEP is responsible for the initiation of investigations for all contractors and employees who require updated and/or upgraded investigations based on position sensitivity, systems access, or clearance requirements. Though, not a specific requirement of HSPD-12 or FIPS-201, the OSEP complies with all OPM regulations concerning reinvestigation requirements.
12	Page 10, Recommendation 1A	"Document the HSPD-12 related roles and responsibilities of other HUD offices..."	The HSPD-12 program is a Departmental initiative. Personnel security policies and directives related to HSPD-12 and FIPS-201 have been disseminated to all HUD employees via memorandums from the Secretary and his immediate staff. Program office Administrative Officers and OHR personnel have been trained by OSEP on the FIPS-201 PIVI process. If and where necessary OSEP will document specific and/or unique roles and responsibilities concerning other program offices in memorandums of understanding to program office managers.
13	Page 11, Recommendation 1B	"Ensure that personal verification registrars, issuers, and adjudicators fully understand..."	HSPD-12 PIVII training is on going. Field office personnel are being trained on the use of SecurityManager. SecurityManager is HUD's new identity management system (IDMS) used to process PIV applicants. The PIVII roles and

Page 6

Comment 11

Comment 12

Comment 13

No	Reference	Audit Report Statement	ADMIN Comment
			responsibilities are system processes within the IDMS. The IDMS requires registrars to verify the applicants' identity documents as specified in FIPS-201. If the applicants do not produce the required identity documents, the enrollment process cannot continue. Registrars must follow the business rules of the IDMS enrollment process and the system will not allow any deviation from that process.
14	Page 11, Recommendation 1C, 1st bullet	"Reflect all federal personal identity verification requirements, including the need to require that HUD officials initiate..."	HUD published the Personal Identity Verification (PIV-I), Part 1 for Federal Employees and Contractors guidance which specifies on page 12, section 2.3, Background Investigation Requirements, that "At a minimum, the National Agency Check (NAC) portion of the NACI must be completed prior to the issuance of any credential. The NAC consists of a search of the OPM Security/Suitability Investigations Index (SII); the FBI's arrest records; and the FBI's investigations records that include a National Criminal History Fingerprint Check (FBI/FP Check). The NAC is initiated by the OPM after HUD sends and the OPM receives the electronic file transfer of the applicants' fingerprint files. Receipt of the fingerprint files by the OPM signifies the initiation of a background investigation.
15	Page 11, Recommendation 1C, 2nd bullet	"Update and/or remove policies no longer in practice, such as revoking building and system access if background investigations are not completed in six months..."	The OSEP will update HSPD-12 policies and procedures to reflect the change in the requirement for the six-month credential revocation period. FIPS201-1 no longer requires the six-month revocation period. The OSEP will ensure that a suitable process is put in place to revoke credentials if background investigations are not completed within a reasonable timeframe.
16	Page 11, Recommendation	"Define the roles and responsibilities of	See item #12 above.

Page 7

Comment 14

Comment 15

Comment 16

No	Reference	Audit Report Statement	ADMIN Comment
	1C, 3rd bullet	other HUD offices..."	
17	Page 11, Recommendation 1D	"Complete its review and verification of information in HUD's paper-based..."	There is no HSPD-12 or FIPS-201 requirement to review and verify information in the paper-based process. If and where necessary OSEP will document specific and/or unique roles and responsibilities concerning other program offices in memorandums of understanding (MOU) to program office managers. For instance, OSEP is working with the OCIO to provide the service as an independent certification agent responsible for monitoring the HSPD-12 program. A MOU is in draft.
18	Page 11, Recommendation 1E	"Develop a strategy to identify and complete background..."	The OSEP has had a strategy in place prior to October 2005 to ensure that all HUD employees and contractors have at a minimum a National Agency Check with Written Inquires (NACI) investigation on file.
19	Page 11, Recommendation 1F	"Verify whether other HUD offices will initiate investigations..."	The OSEP is responsible for the initiation of investigations for all contractors and employees who require updated and/or upgraded investigations based on position sensitivity, systems access, or clearance requirements. Though, not a specific requirement of HSPD-12 or FIPS-201, the OSEP complies with all OPM regulations concerning reinvestigation requirements.
20	Page 12, Finding 2, 1st paragraph, 2nd sentence	"We determined that (1) new systems were placed into production before...(2) the systems currently supporting HUD's personal identity...(3) the initial certification and accreditation of HUD's personal identity...(4) HUD has 14 systems with security categorizations rated as low"	1. The new system, SecurityManager IDMS is not in production and is in fact operating in a pilot mode. The IDMS is currently in the process of receiving its certification and accreditation by an independent OCIO contractor. 2. SCATS is a Microsoft Access database used in the Personnel Security Branch to track the status of background investigations. SCATS is not FIPS-201 compliant and was only used to support the PIVI

Page 8

Comment 17

Comment 18

Comment 19

Comment 20

No	Reference	Audit Report Statement	ADMIN Comment
			process. This particular system was initially created in the OIG Personnel Security office, then moved to the OHR and finally inherited by the Personnel Security Branch in OSEP. This legacy database is password protected and resides on a HUD standard network drive shared only by OSEP personnel authorized to access the data. The data is backed up by the OCIO/HITS data backup procedures. This system is in the process of being phased out. The WinDSX Access Control System (DSX) was not used to support the PIV-I process. The DSX system does not create nor support PIV credentials. DSX is another legacy system inherited from the OAMS and is used solely to manage the HUD ID badges issued to employees and contractors requiring access to HUD facilities. DSX is not FIPS-201 compliant and does not serve in the FIPS-201 PIV program. This system is also being phased out and should not be evaluated in this audit report. 3. OSEP is working with the OCIO to provide the service as an independent certification agent responsible for monitoring the HSPD-12 program. The OCIO will conduct the annual certification and accreditation service as required in FIPS-201. A MOU is in draft. 4. Only systems relevant to HSPD-12 and FIPS-201 should be addressed in this audit report.
21	Page 13, "HUD Placed a New Systems into Production..." 1st paragraph, 1st sentence	"HUD's new Identity Management System, which is currently in pilot phase, is being used to issue identity credentials..."	**No** PIVII identity credentials were issued to headquarters employees.
22	Page 13, "HUD Placed a New Systems into Production..." 1st	"For instance, the Office of Emergency Planning and Management placed a new, automated fingerprint system..."	The CrossMatch 700 fingerprint system is an OPM approved device required by the OPM to submit electronic fingerprint files to the OPM for the

Comment 21

Comment 22

Page 9

No	Reference	Audit Report Statement	ADMIN Comment
	paragraph, 2nd sentence		initiation of background investigations. It is the OSEP understanding that this particular system has been certified and accredited (C&A) by the OPM. The OSEP is in the process of acquiring documentation of the C&A.
23	Page 13, "HUD Placed a New Systems into Production..."2nd paragraph, 1st sentence	"HUD began issuing identity credentials to headquarters employees on June 11, 2007..."	The OSEP has not issued any PIVII identity credentials. On or about June 11, 2007 the OSEP began processing employees and contractors using the new IDMS.
24	Page 14, "The Systems Currently Supporting HUD's Personal Identity..."1st paragraph	"The Office of Security and Emergency Planning did not certify and accredit the systems that currently support...(DSX card management system and Security Control and Tracking System)..."	The DSX Access Control System (DSX) or DSX card management system was not used to support the PIV-I process. The DSX system does not create nor support PIV credentials. DSX is not FIPS-201 compliant and does not serve any roll in the FIPS-201 PIV program. SCATS is a Microsoft Access database used by the Personnel Security Branch to track the status of background investigations. SCATS is not FIPS-201 compliant and was only used to support the PIVI process. This system was initially created in the OIG Personnel Security office, then moved to the OHR and finally inherited by the Personnel Security Branch in OSEP. This legacy database is password protected and resides on a HUD standard network drive shared only by OSEP personnel authorized to access the data. The data is backed up by the OCIO/HITS data backup procedures. This system is in the process of being phased out. Both SCATS (P120) and DSX ((P206) are included in HUD's Inventory of Automated Systems (IAS) and are both categorized as low impact systems.
25	Page 14, "The Systems Currently Supporting	"HUD's Information Technology Security Policy Handbook notes that program	Both SCATS and DSX are legacy systems inherited by the OSEP. Neither system is FIPS-201

Page 10

Comment 23

Comment 24

Comment 25

No	Reference	Audit Report Statement	ADMIN Comment
	HUD's Personal Identity..."2nd paragraph	offices and system owners are responsible for the certification and accreditation..."	compliant. Both of these systems are being phased out. The OSEP will work closely with the OCIO to fully understand the security responsibilities as system owners of the new IDMS and other OSEP systems where applicable.
26	Page 14,"Information Systems Currently Supporting...Were Not Backed Up..."1st paragraph, 2nd sentence	Data contained in the Security Control Action Tracking system were not backed up..."	Should be Security Control and Access Tracking System (SCATS). When the OSEP inherited SCATS from the OHR, SCATS was running on a standalone Intel 386 PC. The OSEP took the steps necessary to put SCATS on the HUD standard LAN file server for additional security and to ensure that the SCATS database would be backed up in accordance to the OCIO LAN backup procedures. The DSX card management system is also a standalone application running on a dedicated network in HUD headquarters. The PC hosting the system is locked up in a secure closet with card reader controls in place. The data in the DSX system is backed internally and to a second PC workstation in a separate secure area on that same dedicated network. Although the backup process indicated some consistencies, there were at a minimum five (5) separate full backup files of the active database.
27	Page 15,"The Initial Certification and Accreditation of HUD's Personal Identity..."1st paragraph	Although HUD's personal identity verification process was certified by the Office of the Chief Information Officer and accredited by the assistant secretary for administration, the certification and accreditation are incomplete because the systems that support..."	Both SCATS and DSX are legacy systems inherited by the OSEP. Neither system is FIPS-201 compliant. Neither system is required or necessary to support the FIPS-201 PIVI process. Both of the systems are being phased out. The OSEP will work closely with the OCIO to fully understand the security responsibilities as system owners of the new IDMS and other OSEP systems where applicable.

Comment 26

Comment 27

Comment 28

Comment 29

Comment 30

Comment 31

No	Reference	Audit Report Statement	ADMIN Comment
28	Page 15,"The Initial Certification and Accreditation of HUD's Personal Identity..."2nd paragraph	"The Office of Security and Emergency Planning was not aware of the requirement to certify and accredit..."	The OSEP was fully aware that a C&A of the SecurityManager IDMS is required prior to releasing the system into HUD's production environment. The OSEP did not have the funding resources necessary to acquire a contractor to perform an independent C&A of the IDMS. The OCIO offered to take on the responsibility to provide the C&A services for the IDMS. OSEP is also working with the OCIO to provide the service as an independent certification agent responsible for monitoring the personal identity verification process. The OCIO will conduct the annual re-certification and accreditation service as required in FIPS-201. A MOU is in draft.
29	Page 16, Recommendation 2A	"Ensure that HUD's personal identity verification process and new Identity Management System, including all components..."	The C&A of the SecurityManager IDMS is in process. The IDMS will not be released into production until the C&A is complete and the system is released through the OCIO software release process.
30	Page 16, Recommendation 2B	"Ensure that system owners fully understand their security responsibilities..."	The OSEP will work closely with the OCIO to fully understand the security responsibilities as system owners of the new IDMS and other OSEP systems where applicable.
31	Page 16, Recommendation 2C	"Ensure that the systems currently supporting HUD's personal identity verification system..."	The legacy systems SCATS and DSX are not FIPS-201 compliant and are being phased out and replaced by the new IDMS. The databases of both systems were backed up to separate servers and hard drives prior to the data migration to the IDMS. Access to the backed up data was fully tested as well. The IDMS is in its final C&A phase. Once the C&A is granted by the OCIO, the OSEP will begin the process to release the system into production. Once released into the production environment, the IDMS will be backed up by the OCIO standard LAN backup procedures.

Page 12

OIG Evaluation of Office of Security and Emergency Planning (OSEP) Comments

Comment 1: OIG agrees and has removed the phrase "will not meet all remaining implementation deadlines" from the final report.

Comment 2: We mentioned in the report, that HUD has published PIV guidance and provided training to staff in support of the PIV-I process. However, during our review, we identified 46 instances where policies and procedures were not followed. Because HUD did not monitor its PIV process, these irregularities went undetected and uncorrected.

PIV-I involves only the personal identity proofing process, which can be either role-based or system based. While HUD's "system based" process should greatly reduce the chance for human error, HUD must continue to monitor its PIV process.

Comment 3: OIG disagrees. Regardless of the origin of the systems, the fact is that OSEP has been the owner of SCATS and DSX for several years but did not take action to assure the security status of these systems. OMB Circular A-130, Appendix III requires the security accreditation of all information systems. NIST SP 800-37 specifically notes that this requirement also applies to legacy systems. Further, neither OSEP nor OCIO was able to provide documentation to OIG to support that SCATS data and application files were regularly backed up. As stated in the privacy impact assessment for HUD's PIV process and confirmed by OSEP officials during our review, the DSX is used in conjunction with IDMS to verify, authenticate, and revoke PIV cardholder access to federal facilities (buildings and office space). Thus, the system is part of HUD's PIV process. Additionally, one of our audit objectives was to evaluate HUD's privacy program. Both DSX and SCATS contain PII data. Therefore, OSEP should ensure that adequate security controls are in place for DSX and SCATS regardless of whether they support the PIV process.

Comment 4: OIG agrees with the Department's comment and commends its willingness to make the recommended changes.

Comment 5: OIG disagrees. The systems currently supporting HUD's PIV process were not certified and accredited. Because of this, the certification of HUD's PIV process was incomplete. Additionally, a component of HUD's new IDMS was placed into production without being certified and accredited.

Comment 6: OIG agrees and has added language to the final report to reflect that OCIO is responsible for the logical access portion of HSPD 12.

Comment 7: See OIG's responses to comment #2 above and comment #9 below.

Comment 8: The automated systems that support HUD's current personal identity verification process have limited reporting capabilities, so HUD could not easily provide the information we requested. As a result, we were unable to obtain the universe of employees, contractors, or identification badges issued. Also, OSEP management's ability to monitor and manage ID badges issued to employees and contractors were limited by the paper based process.

Comment 9: OIG disagrees and notes that OSEP is mistaken in its interpretation of the requirements. FIPS 201, section 2 states that "PIV-I addresses the fundamental control and security objectives outlined in HSPD 12, including the personal identity proofing process for employees and contractors." OMB Memorandum M-05-24 further notes that agencies must adopt the identity proofing and registration process noted in FIPS 201 section 2 **regardless** of whether they will be ready to issue standard compliant identity credentials. OSEP has mistakenly assumed that PIV-II is separate and apart from PIV-I. In actuality PIV-I is the identity proofing, registration and verification process, while PIV-II refers to the components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical and logical access environments. All personal identity proofing, registration and verification activities associated with PIV-I MUST be completed before either an identification badge OR credential can be issued. We evaluated HUD's PIV-I process for identity proofing, registration and verification, which, according to HUD, has been in place since October 2005.

Comment 10: OIG disagrees. During the review, OSEP did not provide support to show that regular reviews of the PIV-I paperwork were conducted weekly by randomly selecting enrollment documents and checking them for accuracy and compliance to the PIV-I requirements. Even if such reviews were done, there is no evidence that feedback was provided to ensure that the same mistakes were not repeated. As noted in our report, we identified 46 instances of non-compliance with policies and procedures.

Comment 11: Based on additional information provided by OSEP, OIG agrees and has removed this language from the final report.

Comment 12: We commend OSEP for working with other offices within HUD to help ensure that the requirements of HSPD 12 will be met.

Comment 13: PIV-I is the identity proofing, registration and verification process. While these activities will largely be automated, which should reduce the risk of human error, HUD should continue to train officials in support of the PIV process to ensure

they fully understand the requirements of PIV-I to verify the identity of employees and contractors.

Comment 14: OIG has revised the recommendation to clarify that the requirement to complete the fingerprint check means to receive the results. During our review, we identified 20 instances where identification badges were issued before the fingerprint check was completed.

Comment 15: OIG agrees with the Department's comment and commends its willingness to make the recommended changes.

Comment 16: OIG agrees with the Department's comment and commends its willingness to make the recommended changes.

Comment 17: We commend the Department for taking steps to appoint an independent certification agent to monitor the HSPD 12 program as required by NIST SP 800-79.

Comment 18: OIG agrees and has removed this recommendation from the final report.

Comment 19: OIG agrees and has removed this recommendation from the final report.

Comment 20: While the comments provided are explanatory in nature, they do not change the facts included in our audit report.

(1) Although OSEP officials state that the new system is operating in pilot mode, it is still being used for the PIV process in preparation for the issuance of HUD identity credentials. Further, the Cross Match 700, an automated fingerprinting system, has been in use for several months even though it has not been certified and accredited.

(2) Regardless of the origin of the systems, the fact is that OSEP has been the owner of SCATS and DSX for several years but did not take action to certify and accredit these systems. OMB Circular A-130, Appendix III requires the security accreditation of all information systems. NIST SP 800-37 specifically notes that this requirement also applies to legacy systems. Although HUD is not yet issuing identity credentials, DSX was used in the PIV process to manage HUD ID badges. Thus, it was part of HUD's PIV process at the time of our review. During our review, OSEP officials were unable to support their response that data and application files for systems supporting the PIV process were backed up in accordance with NIST and Departmental guidelines.

(3) We commend OSEP for working with other offices within HUD to help ensure that the requirements of HSPD 12 will be met.

4) As we mentioned in our responses to comment 3, one of our audit objectives was to evaluate HUD's privacy program. Both DSX and SCATS contain PII data. Therefore, OSEP should ensure that adequate security controls are in place for DSX and SCATS regardless of whether they support the PIV process.

Comment 21: According to the HUD ID Badge Rollout Schedule, published June 13, 2007, HUD began issuing new Federal ID credentials to Headquarters employees on June 11, 2007. However, based on prior discussions with OSEP officials, we will change the wording to reflect that the new system is being used in HUD's PIV process in preparation for issuing new ID badges and identity credentials.

Comment 22: Even if the Cross Match 700 had been certified and accredited by OPM, further analysis would be necessary to ensure that the system operates securely and effectively in the HUD environment. During our review, OSEP officials were not able to provide support to show that any type of security analysis in HUD's environment was performed for the Cross Match 700.

Comment 23: OIG agrees and has changed the wording in the final report to reflect that OSEP began processing employees and contractors using the new IDMS.

Comment 24: OIG disagrees. See response to comment # 20. During the review, OSEP officials informed us that they did not report DSX to OCIO to be included in IAS because DSX is a small system and is not supported by OCIO. OSEP did not provide the system code P206 to OIG until August 6, 2007. We reviewed information in IAS for P206 but were unable to confirm if this was actually the system in question because the system name is different and the description is very brief. Also, according to NIST SP 800-60, the systems should be categorized as moderate impact because they contain sensitive, PII data.

Comment 25: We commend OSEP for taking steps to ensure that security responsibilities are fully understood. However, regardless of the origin of the systems, the fact is that OSEP has been the owner of SCATS and DSX for several years but did not take action to certify and accredit these systems.

Comment 26: We have changed the language in the final report to reflect the correct name of the system. However, neither OSEP nor OCIO was able to provide documentation to OIG to support that SCATS data and application files had been backed up during the review. Also, OSEP officials did not review or test the backup information periodically to ensure media reliability and information integrity. When we reviewed the backup information for DSX on June 8, 2007, we found that the data was only backed up three times from October 12, 2006 to June 2, 2007.

Comment 27: We disagree with OSEP's response that neither SCATS nor DSX support the PIV-I process. During our review, we confirmed that both systems were used as part of the PIV process. The fact remains that neither system was certified or accredited. We are pleased that OSEP plans to work closely with OCIO to fully understand its security responsibilities as system owners.

Comment 28: The statement in question refers to the systems currently supporting HUD's PIV process, not the new IDMS. We commend OSEP for arranging for the

certification and accreditation of its new IDMS, and for taking steps to establish a formal agreement for annual re-certification and accreditation.

Comment 29: OIG agrees.

Comment 30: OIG agrees.

Comment 31: See response to comment #26. OIG commends OSEP for taking immediate corrective actions and requests that OSEP provide documentation to support completion of these actions.

Appendix B

Office of the Chief Information Officer (OCIO) COMMENTS AND OIG'S EVALUATION

No	Reference	Audit Report Statement	OITS Comment
1	Page 2, "What We Recommend", 2nd paragraph, 1st sentence	"We recommend that the Office of the Chief Information Officer ensure that (1) systems with personally identifiable information are categorized properly by program offices…"	This finding should be directed at program offices since the OCIO has no enforcement powers over program offices, has taken appropriate steps to educate program office system owners on the categorization process, and continues to monitor the system categorization process.
2	Page 2, "What We Recommend", 2nd paragraph, 2nd sentence	"We recommend that the Office of the Chief Information Officer ensure that (2) all HUD systems comply with backup requirements stated in NIST SP 800-53, especially systems with moderate and high impact levels."	This finding should be directed at the Office of Security and Emergency Planning since it failed to comply with NIST SP 800-53 backup controls stipulated in HUD's IT Security Policy while conducting the pilot of the IDMS in a standalone mode outside the HITS infrastructure.
3	Page 8, "HUD Did Not Monitor Its Personal Identity Verification Process", 2nd paragraph, 2nd sentence	"…there was no formal agreement between the offices for this service, and responsibility for certifying and monitoring the PIV process was never documented or formally established."	NIST SP 800-79 documents and establishes the responsibility of the system owner in certifying and monitoring the PIV process.
4	Page 12, Finding 2, 1st paragraph, 3rd sentence	"These conditions occurred because personnel responsible for HUD's PIV and privacy program were not aware of all information security requirements and did not fully understand their security responsibilities."	The Office of the CIO has published policy, procedures, and guidance for use by system owners concerning categorization of personally identifiable information, categorization of information systems, certification and accreditation of information systems, and controls for backing up sensitive data.
5	Page 13, HUD Placed a New Systems into Production Before Full Certification Testing Was Completed, 1st paragraph, 1st sentence.	"HUD's new IDMS, which is currently in pilot phase, is being used to issue identity credentials to headquarters employees."	The IDMS is not in production and is in fact operating in a pilot mode. No identity credentials have been issued to headquarters employees, and current HSPD-12 project planning calls for credentials to be issued only when the IDMS has been certified and accredited.
6	Page 15, The Initial C&A of HUD's PIV Process Was Incomplete and Expired in April 2007., 2nd paragraph, 1st sentence	"OSEP was not aware of the requirement to certify and accredit the PIV system in conjunction with the PIV process."	See comment #4 above
7	Page 15, The Security Impact Level of 14 Systems Containing PII Was Understated,	"HUD has 14 systems with security categorizations rated as low impact that contain PII."	There is no federal requirement that systems processing PII be categorized at a specific level. System owners categorize their systems IAW FIPS 199 using NIST SP 800-60 as guidance and are permitted to categorize systems that process PII at either the high, moderate, or low level based on the risk impact to PII data.
8	Page 16, Recommendation 2D	"Ensure that information system owners receive information security training to ensure compliance with federal and HUD-issued information security requirements."	The OCIO has done and continues to provide system owners with training relevant to their security duties.
9	Page 16, Recommendation 2E	"Ensure that system owners comply with federal and HUD-issued requirements to back up systems and data, particularly those systems with moderate and high security impact levels.	This finding should be directed at program offices since the OCIO has no enforcement powers over program offices, has taken appropriate steps to educate program office system owners on requirements for implementing controls to include those relating to the back-up of sensitive data.
10	Page 16,	"Update its IT Security Policy	See comment #7 above

No	Reference	Audit Report Statement	OITS Comment
	Recommendation 2F	Handbook to specify that systems with PII should be categorized as moderate or high impact."	
11	Page 16, Recommendation 2F	"Notify system owners identified as having systems with security categorizations rated as low impact that contain PII and instruct them to update the security categorizations."	See comment #7 above

OIG Evaluation of OCIO's Comments

Comment 1: We disagree. The HUD Chief Information Officer (CIO) is responsible for establishing policy and oversight procedures to oversee the department-wide Information Security Program and provide consulting assistance to all HUD program offices. HUD's Information Technology Security Policy does not provide specific instructions to program offices to categorize systems containing PII as moderate or high impact level. After program offices categorize their systems, OCIO should review supporting documents to ensure they are in compliance with federal and HUD IT security requirements.

Comment 2: We disagree. HUD's Information Technology Security Procedures notes that both deputy CIO for IT operation and Program office/system owners are responsible for ensuring HUD systems are compliance with backup requirements.

Comment 3: We disagree. NIST 800-79 requires an independent certification agent be appointed to perform certifications (i.e., comprehensive assessments) of a PIV card issuing organization. To preserve the impartial and unbiased nature of certifications, the certification agent should be independent of, and organizationally separate from, the persons and the office(s) directly responsible for the day-to-day operation of the PIV card issuing organization. While OCIO does not have to continue to be the certification agent, we recommended in the report that OSEP, not OCIO, should select a new certification agent from another program office and document the roles and responsibilities in HUD's policies or in formal agreements.

Comment 4: We agree that OCIO has published policies, procedures and guidance to outline system owners' roles and responsibilities. However, since key personnel within OSEP informed us during our review that they were not aware of all information security requirements, we recommended that OSEP, not OCIO, ensure system owners fully understand their security responsibilities.

Comment 5: We disagree. According to the HUD ID Badge Rollout Schedule, published June 13, 2007, HUD began issuing new Federal ID credentials to Headquarters employees on June 11, 2007. OSEP officials have acknowledged that the new IDMS is currently being used in the PIV process for these new identity credentials. Since OSEP is the program/system owner, it is in a better position to know the status of its program and system. Further, the new automated fingerprint system (Cross Match 700) has been in use for several months even though it has not yet been certified and accredited.

Comment 6: We disagree. During our review, we confirmed that neither OSEP nor OCIO personnel were aware that NIST SP 800-79 requires that the security of systems supporting the PIV process must be certified and accredited in conjunction with the certification and accreditation of the PIV process. This is necessary to establish the reliability of a PIV card issuing organization. In addition, these requirements outlined in NIST 800-79 are not included or referenced in OCIO's current policies procedures and guidance.

Comment 7: We disagree. Based on the definitions and guidance from OMB memorandums, the Privacy Act and the Computer Security Act, it is clear that PII is sensitive, Privacy Act-protected information. NIST SP 800-60 states that the security categorization will generally be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review. NIST SP 800-60 also notes that in most cases, for systems containing privacy information, the impacts will fall into the moderate range.

Comment 8: See OIG's responses to comment 4 above. OCIO should ensure all system owners are informed of and receive the specialized trainings provided by OCIO.

Comment 9: See OIG's responses to comment 2 and comment 4 above.

Comment 10: See OIG's responses to comment 7 above.

Comment 11: See OIG's responses to comment 7 above.

Appendix C

Office of the Chief Procurement Officer (OCPO) COMMENTS AND OIG'S EVALUATION

Office of the Chief Procurement Officer
Draft Audit Report Comments
Review of HUD's Personal Identity Verification and Privacy Program
August 10, 2007

Reference: OIG memorandum (GAA) dated July 23, 2007, subject: Draft Audit Report Review of HUD's Personal Identity Verification and Privacy Program

Page 9: HUD's Contracting Officers Did Not Always Include Contract Language to Implement the Personal Identity Verification Requirements of HSPD 12

Comment 1

- **First bullet:** OCPO managers finalized the two modifications awaiting management approval.

Comment 2

- **Second bullet:** The reference to the one contract with an outdated personnel security clause should be deleted and/or restated. Per discussions with OIG and OCPO, it was determined that the contract in question does not require the contractor to have access to HUD facilities and/or systems. All work is done off-site at the Contractor's facility and routine access to HUD facilities is not required nor does the Contractor require access to any HUD systems/applications. Therefore, the inclusion of the outdated clause was inadvertent as it was not required for the contract work effort.

Page 10: We recommend that the Office of the Chief Procurement Officer:

1G: Develop a process to ensure that contracting officers include contract language to implement HSPD-12 standards for all applicable new and existing contracts.

Comment 3

OCPO Comments: HUD Acquisition Regulation sections 2437.1 and 2439.10 clearly prescribe the use of HSPD-12-related clauses. For the short term, Supervisory Contract Specialists and Contracting Officers will emphasize to their subordinate Contract Specialists the responsibility to follow existing procurement regulations by including the clauses as applicable. OCPO managers will monitor compliance/quality control of contract content to ensure compliance with the HUDAR through the use of review checklists, etc. In addition, these managers agree to conduct compliance reviews of existing contracts for inclusion of HSPD-12 clauses as applicable not later than **December 15, 2007**.

For the long term, OCPO seeks to acquire a new web based procurement system designed with query capability features that will provide data on contracts that require compliance with HSPD-12 and other statutory/regulatory mandates.

Comment 4

Office of the Chief Procurement Officer
Draft Audit Report Comments
Review of HUD's Personal Identity Verification and Privacy Program
August 10, 2007

1H: Develop a mechanism to readily identify contracts where access to federally controlled facilities and/or information systems will be required.

OCPO Comments:

Coordination with the OSEP revealed that OSEP captures data on the issuance of credentials associated with granting of access to HUD facilities and/or systems. Further, OSEP indicated information can be provided on granting of access in a number of ways, to include contract numbers. The OSEP captured information appears adequate to identify contracts where access to HUD controlled facilities and/or information systems were granted.

Contaminant with contract award, Contracting Officers designates Government Technical Representatives (GTRs) responsibility to facilitate oversight of contractor performance. The GTR coordinates directly with OSEP in order to acquire access authorization on behalf of the Contractor to HUD facilities and/or systems. The GTR secures OSEP required documentation for completion by contractor personnel and provides it to OSEP for processing and issuance of required credentials and access authorization to HUD systems/applications.

OIG Evaluation of OCPO's Comments

Comment 1: OIG commends the Department for taking actions to ensure contracting officers include HSPD 12 requirements in applicable existing contracts when contract options are exercised.

Comment 2: OIG initially reported two contracts awarded after October 27, 2005 as exception items. One contract did not include the HSPD-12 security clause, while the other contract contained an outdated security clause. OCPO provided documentation to show that the first contract did not require the HSPD 12 security clause since the contractor did not require building or system access. The contractor in the second contract did require building and/or system access. Consequently, during our meeting on May 23, 2007, OCPO agreed to initiate a contract modification to replace the outdated security clause with the current HSPD 12 clause. The outdated security clause was dated January 2002; HSPD 12 was enacted in August 2004.

Comment 3: OIG agrees with the Department's comment and commends its willingness to make the recommended changes.

Comment 4: OIG notes that the Department's comment is an appropriate step and suggests that OCPO continue working with OSEP and GTRs to identify all contracts in which access to federally controlled facilities and/or information systems will be required.