OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

THE SOCIAL SECURITY ADMINISTRATION'S
PROGRESS IN IMPLEMENTING
HOMELAND SECURITY
PRESIDENTIAL DIRECTIVE 12

July 2007 **A-14-07-27110**

AUDIT REPORT

Mission

By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.

SOCIAL SECURITY

MEMORANDUM

Date: July 26, 2007 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Progress in Implementing Homeland Security Presidential Directive 12 (A-14-07-27110)

OBJECTIVE

Our objective was to determine the Social Security Administration's (SSA) progress in implementing Homeland Security Presidential Directive (HSPD) 12 as of October 27, 2006.

BACKGROUND

On August 27, 2004, the President of the United States signed HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors.* HSPD-12 directed the promulgation of a Federal standard for a secure and reliable form of identification for Federal employees and contractors.

To assist in the implementation of HSPD-12, the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standard (FIPS) Publication (PUB) 201.[1] FIPS PUB 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* provides guidance that executive departments and agencies are to use to implement HSPD-12. FIPS PUB 201-1 (the "Standard") is to be implemented in two parts. Part-I addresses control and security objectives and Part-II addresses the technical components and processes that support a common smart card-based platform.

[1] FIPS PUB 201, PIV of Federal Employees and Contractors, was amended in March and June of 2006. After the March 2006 amendment, the publication reference number became 201-1.

The Office of Management and Budget (OMB) issued Memorandum M-05-24 on August 5, 2005.[2] M-05-24 provides implementing instructions and timelines for additional actions that Federal departments and agencies need to complete for HSPD-12 by certain specified dates. For example, the Memorandum indicates that all covered Federal Departments and agencies must:

- adopt and accredit a registration process consistent with FIPS PUB 201 identity proofing, registration and accreditation requirements for new Agency employees, contractors and other applicable individuals by October 27, 2005;[3]

- begin deploying products and operational systems by October 27, 2006, to issue and require the use of identity credentials for all new employees and contractors, compliant with Part 1 and Part 2 of the Standard. For current employees and contractor personnel, phase in issuance and use of identity credentials meeting the Standard no later than October 27, 2007;[4]

- plan for and begin background investigations for all current employees with 15 years or less Federal service and current contractor personnel who do not have an initiated or successfully adjudicated investigation on record. Verification and/or completion of background investigations for all current employees are required by October 27, 2007, as is the phase-in of a plan and initiation of investigations for all current contractors;[5] and

- complete new background investigations, commensurate with risk, for all Department or agency employees with over 15 years Federal service no later than October 27, 2008.[6]

FIPS PUB 201-1 indicates that all departments and Agencies shall implement the Personal Identity Verification (PIV) system in accordance with the spirit and letter of all privacy controls specified in that standard as well as those specified in Federal privacy

---

[2] OMB Memorandum M-05-024, *Implementation of Homeland Security Presidential Directive 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*.

[3] OMB, Memorandum M-05-24, Attachment A § 3.A., p. 5.

[4] OMB, supra, § 4, p. 6.

[5] OMB, supra, § 3.D and 3.E., p. 6.

[6] OMB, supra, § 3.D, p. 6.

laws and policies, including but not limited to the E-Government Act of 2002[7] (E-Gov), the Privacy Act of 1974,[8] and OMB Memorandum M-03-22,[9] as applicable.[10]

RESULTS OF AUDIT

SSA had implemented a number of important OMB and FIPS PUB 201-1 requirements for HSPD-12 as of October 27, 2006. For example, SSA:

- Created and used an HSPD-12 identity proofing, registration and issuance process for new Agency employees hired at its Headquarters (HQ) complex.
- Issued 13 PIV II credentials before the OMB mandated target date.
- Formulated and executed a plan to help ensure that SSA employees have an appropriate background investigation either initiated or on file.
- Filed the required notices and took appropriate actions needed to address HSPD-12 privacy and security requirements involving the protection of Personally Identifiable Information in the development of a new system of records.

However, SSA needs to address the following areas:

- SSA's HSPD-12 identity proofing, registration, and issuance process was not implemented nationwide.
- SSA contractor personnel hired during the period of October 27, 2005 through October 27, 2006 were not processed using the SSA HSPD-12 identity proofing and registration protocol.
- The General Services Administration (GSA) found that SSA credentials were not fully compliant with technical requirements.
- The infrastructure needed to support the use of the credentials issued was not in place due to GSA delays.

---

[7] 44 U.S.C. ch. 36.

[8] 5 U.S.C. § 552a.

[9] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.

[10] U.S. Department of Commerce, Federal Information Processing Standard (FIPS) 201-1, Section 2.4, p. 7, March 2006.

THE SSA PERSONAL IDENTITY PROOFING, REGISTRATION, AND ISSUANCE PROCESS WAS NOT IMPLEMENTED NATIONWIDE

The personal identity proofing, registration and issuance process adopted by SSA was not implemented nationwide. Therefore, new SSA employees hired outside of the HQ complex were not processed in accordance with SSA's HSPD-12 personal identity proofing and registration protocol. As a result, SSA may not have achieved HSPD-12 objectives to enhance security and increase Government efficiency with respect to employees hired outside the HQ complex during the review period of October 27, 2005 to October 26, 2006. FIPS PUB 201-1[11] requires the adoption and use of an HSPD-12 identity proofing and registration process that satisfies Part 1 PIV I control and security objectives (for details see report Appendix B-2, Section titled *Control Objectives for HSPD-12*).

According to Agency management, the scarcity of resources and tight time constraints limited implementation of a compliant HSPD-12 standard personal identity verification system. SSA needs to expand this process nationwide for all new employees.

NEW CONTRACTOR PERSONNEL WERE NOT PROCESSED USING THE SSA HSPD-12 IDENTITY PROOFING AND REGISTRATION PROTOCOL

New contractor personnel hired during the review period of October 27, 2005 to October 26, 2006 were not processed in accordance with the required SSA HSPD-12 identity proofing and registration protocol. As a result, SSA may not have achieved HSPD-12 objectives to enhance security and increase Government efficiency with respect to new contractor personnel hired. FIPS PUB 201-1[12] requires the adoption and use of an HSPD-12 identity proofing and registration process that satisfy Part 1 PIV I control objectives (for details see Appendix B-2, Section titled *Control Objectives for HSPD-12*).

According to SSA management, formal guidance was not initially available in the review period that would have enabled the Agency to develop a process that would meet HSPD-12 contractor personnel processing requirements. GSA, in November 2006, issued a new Federal Acquisition Regulations Clause[13] that addressed HSPD-12 compliance. SSA needs to modify future contract language where appropriate and use HSPD-12 identity proofing and registration protocol to process new SSA contractor personnel.

---

[11] FIPS 201-1, supra, Section 2.2 requires the adoption and use of an approved HSPD-12 identity proofing and registration process, to satisfy PIV I control objectives (for details see report Appendix B-2 Section titled Control Objectives for HSDP-12).

[12] Id.

[13] Federal Acquisition Regulations *subpart 52.2 Text of Provisions and Clauses*, *52.204-9 Personal Identity Verification of Contractor Personnel,* (November 2006).

PIV II CREDENTIALS ISSUED WERE NOT CERTIFIED AND INFRASTRUCTURE WAS NOT IN PLACE

SSA issued thirteen PIV II credentials prior to the mandated target date for beginning to deploy such products. However, those credentials were not certified by GSA as meeting FIPS PUB 201-1 credential technical requirements.[14] Additionally, the infrastructure necessary to support the use of the issued credentials was not in place. Therefore, while SSA demonstrated the ability to issue a PIV credential, the credential issued did not fully meet HSPD-12 credential technical requirements. OMB Memorandum M-05-24 requires implementation of Part 2 of the Standard by mandating that by October 27, 2006, all Federal departments and agencies begin deploying products and operational systems meeting certain requirements, including issuing and requiring the use of identity credentials for all new employees and contactors, compliant with Parts 1 and Part 2 of the Standard.[15] Further, OMB Memorandum M-07-06 requires that all agencies must provide to GSA, by January 19, 2007, a credential with their agency's standard configuration for testing to ensure that the agency credential meets FIPS 201-1 requirements.[16]

SSA submitted its HSPD-12 credential to GSA in November 2006 for compliance testing. The results of the November 2006 test were mixed. The SSA credential passed some tests and failed others. SSA management stated that it will resubmit the credential for additional compliance testing when the areas where the credential failed have been addressed.

SSA management also stated that the completion of the SSA HSPD-12 infrastructure is dependent upon GSA's acquisition of the hardware security module and the card management system. When these elements become available, SSA will be able to implement the infrastructure needed to support the use of a compliant HSPD-12 credential nationwide.

SSA should obtain GSA certification for the credential it plans to use to meet HSPD-12 technical operability requirements and when available, implement the infrastructure needed to support the use of Part 2 compliant credentials.

---

[14] FIPS 201-1, supra, Part 2: PIV-II, provides detailed information as to the technical functional requirements that the PIV II credential needs to meet (see Sections 4.1 through 4.5.3, pages 15-37).

[15] OMB, supra, § 4, p. 6.

[16] OMB Memorandum M-07-06, § 1.

CONCLUSIONS AND RECOMMENDATIONS

SSA had implemented a number of important OMB and FIPS PUB 201-1 requirements for HSPD-12 as of October 27, 2006. For example, SSA created and used an HSPD-12 identity proofing, registration and issuance process for new Agency employees at its HQ complex; issued 13 PIV II credentials before the OMB mandated target date; formulated and executed a plan to help ensure SSA employees have an appropriate background investigation initiated or on file; and filed the required notices and took appropriate actions needed to address HSPD-12 privacy and security requirements involving the protection of Personally Identifiable Information in the development of a new system of records.

However, SSA still needs to: implement an HSPD-12 identity proofing, registration, and issuance process nationwide and use it to process new SSA employees and contractor personnel; issue a credential that has been certified by NIST as having met Part 2 PIV II credential technical requirements and implement the infrastructure needed to support the use of a compliant credential.

We recommend SSA:

1. Implement the HSPD-12 identity proofing, registration and issuance process nationwide for all new SSA employees and contractor personnel.

2. Ensure contract language is HSPD-12 compliant where appropriate.

3. Issue credentials certified by GSA as having met Part 2 PIV II credential technical requirements.

4. When available, implement the necessary infrastructure that will support and control the use of a compliant credential.

AGENCY COMMENTS

SSA agreed to implement our recommendations. The Agency added that it could not comply with our recommendations in the past due to conditions outlined in the full text of its comments shown in Appendix E. However, SSA plans to implement each of the OIG recommendations in the future.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

E-GOV	Electronic Government
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
GSA	General Services Administration
HQ	Headquarters
HSPD	Homeland Security Presidential Directive
NACI	National Agency Check with Written Inquiries
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PIV	Personal Identity Verification
SSA	Social Security Administration

Background

On August 27, 2004, the President of the United States signed Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (the Directive). HSPD-12 directed the promulgation of a mandatory Federal Government-wide standard for secure and reliable forms of identification for Federal employees and contractors (including contractor employees).

To aid in the implementation of HSPD-12, the National Institute of Standards and Technology (NIST) issued Federal Information Processing Standard (FIPS) Publication (PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors.* FIPS PUB 201-1 provides guidance that executive departments and agencies are to use to implement HSPD-12.

FIPS PUB 201-1 contains 2 parts. Part 1 addresses control and security objectives of the Directive that have a mandated implementation date of October 27, 2005. Part 1 requires the adoption and accreditation of personal identity proofing, registration, and issuance and maintenance process for new employees and contractor personnel. Part 2 addresses the technical components and processes that support a common smart card-based platform for identity authentication across Federal Departments and agencies for access to federally controlled physical and logical environments. Implementation of Part 2 requirements is mandated as of October 27, 2006.

The Office of Management and Budget (OMB) issued Memorandum M-05-24 on August 5, 2005. M-05-24 provides implementing instructions and timelines for additional actions that Federal Departments and agencies should complete for the Directive. For example, the Social Security Administration (SSA) is required to comply with the implementation timeframes set forth below:

AGENCY REQUIRED MILESTONES AND ACTIONS

Date	Agency Action
6/27/05	Implementation plans submitted to OMB
8/26/05	Provide list of other potential uses of the Standard
10/27/05	Comply with FIPS PUB 201, Part 1
10/27/06	Begin compliance with FIPS PUB 201-1, Part 2
10/27/07	Verify and/or complete background investigations for all current employees and contractor personnel
10/27/08	Complete new background investigations, commensurate with risk, for all Federal agency employees who have over 15 years service time

CONTROL OBJECTIVES OF HSPD-12

For purposes of HSPD-12, "…secure and reliable forms of identification…" for Federal employees and contractors means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.[1]

Each agency's PIV-I implementation shall meet the above referenced four HSPD-12 control objectives by ensuring that credentials are issued 1) to individuals whose true identity has been verified and 2) after a proper authority has authorized issuance of the credential. Further, 3) only an individual with a background investigation on record is issued a credential; 4) an individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture ID; 5) fraudulent identity source documents are not accepted as genuine[2] and unaltered; 6) a person suspected or known to the government as being a terrorist is not issued a credential; 7) no substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued; 8) no credential is issued unless requested by proper authority; 9) a credential remains serviceable only up to its expiration date and that a revocation process exists such that expired or invalidated credentials are swiftly revoked; 10) a single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential; and 11) an issued credential is not modified, duplicated, or forged.[3]

PIV IDENTITY PROOFING AND REGISTRATION REQUIREMENTS

Departments and agencies are required to follow an identity proofing and registration process that meets the following requirements when issuing identity credentials:[4]

- The organization shall adopt and use an approved identity proofing and registration process.
- The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI), or other Office of Personnel Management or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully

[1] Homeland Security Presidential Directive/HSPD-12, § (3), August 27, 2004.

[2] FIPS, supra, § 2.2 requires the adoption and use of an approved HSPD-12 identity proofing and registration process, in order to satisfy PIV 1 control objectives.

[3] FIPS, supra, § 2.1, page 5.

[4] FIPS, supra, § 2.2, pages 5-6.

adjudicated NACI. At a minimum, the Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) shall be completed before credential issuance.[5]

- The applicant must appear in-person at least once before the issuance of a PIV credential.
- During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, *Employer Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID).
- The PIV identity proofing, registration and issuance process shall adhere to the principal of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

PIV PRIVACY REQUIREMENTS

To ensure the privacy of applicants, departments and agencies shall:[6]

- Assign a senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard. The person serving in this role cannot assume any other operational role in the PIV system.
- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with the E-Government Act of 2002[7] and OMB Memorandum M-03-22. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.
- Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected, the purpose of the collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. PIV applicants shall be provided full disclosure of the intended uses of the PIV and the related privacy implications.

[5] OMB Memorandum M-05-24 footnote 6, on page 5, indicates that section 2.2 of the Standard has been revised to clarify for the initial credential issuance, that only the fingerprint check must be completed.

[6] FIPS, supra, § 2.4, p. 7-8.

[7] Pub. L. 107-347, 116 Stat. 2899.

- Assure that systems that contain Information in Identifiable Form for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in the Privacy Act of 1974.[8]
- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to Information in Identifiable Form in the PIV system are authorized to access the Information in Identifiable Form including but not limited to information and databases maintained for registration and credential issuance.
- Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.
- Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
- Utilize security controls described in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, to accomplish privacy goals, where applicable.
- Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.

[8] 5 U.S.C. § 552a, as amended.

Scope and Methodology

To determine the progress that the Social Security Administration (SSA) has made in implementing Homeland Security Presidential Directive (HSPD) 12 as of October 27, 2006, we:

- Reviewed applicable laws, regulations and guidance pertaining to HSPD-12.
- Reviewed Agency policies and procedures that were used in implementing HSPD-12 requirements.
- Interviewed appropriate SSA personnel and examined relevant documentation.
- Observed the HSPD-12 credentialing process at the Headquarters' complex.
- Conducted a random sample of SSA new hires in the Baltimore metropolitan area during the period of October 27, 2005 through October 26, 2006.
- Discussed our preliminary results with Agency management responsible for the implementation of HSPD-12.

To meet our objective, we interviewed management and key staff within the SSA Office of Protective Security Services, and Office of Personnel components located at the Office of Central Operations, the Office of Disability Adjudication and Review, and SSA Headquarters' complex. We also observed the process used by the SSA Headquarters' complex Parking and Badging Office to issue badges to Headquarters new hires during the period of October 27, 2005 to October 26, 2006. Our field work was performed from October 2006 through February 2007. This audit was performed in accordance with generally accepted government auditing standards. The review period was October 27, 2005 through October 26, 2006.

Sampling Methodology and Results

We selected a random statistical sample of SSA personnel who were hired in the Baltimore metropolitan area during the period of October 27, 2005 through October 26, 2006. We randomly selected 50 individuals from a population of 698 individuals hired during that time. Our objective was to determine if the SSA identity proofing, registration and issuance process in place met HSPD-12 requirements.

An approved SSA HSPD-12 identity proofing, registration, and issuance process was in place for 21[1] of the 50 individuals sampled. For the remaining 28 individuals, an SSA HSPD-12 identity proofing, registration, and issuance process was not implemented Agency-wide. Through our sample results and interviews with SSA managers, we determined SSA had implemented an HSPD-12 process for 21 individuals who were hired for Headquarters positions. The results are presented in the following table.

Location	Total	Applicant Appeared In-person Before Badge Issued	FBI Fingerprint Check Completed	Background Investigation Completed, Scheduled, not Needed, or in Process	Two Forms of OMB I-9 Documents Obtained	PIV Request Checklist Completed
Headquarters						
	22	19	21	21	19	19
Non-Headquarters						
Office of Central Operations	21	21	21	20	19	0
Office of Disability Adjudication and Review	6	6	6	6	5	0
National Computer Center	1	1	1	1	1	0
Total	**50**	**47**	**49**	**48**	**44**	**19**

[1] One individual hired at the SSA Headquarters complex was a member of the SSA Board of Trustees. As such, this individual would have no need to access SSA controlled facilities or system resources.

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: July 6, 2007 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: David V. Foster (David A. Rust /s/ for)
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Progress in Implementing Homeland Security Presidential Directive-12" (A-14-07-27110)--INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "SOCIAL SECURITY ADMINISTRATION'S PROGRESS IN IMPLEMENTING HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12" (A-14-07-27110)

Thank you for the opportunity to review and comment on the draft report. We appreciate your conducting this audit of the Social Security Administration's (SSA) progress in implementing Homeland Security Presidential Directive (HSPD)-12 for the period October 27, 2005 through October 2006.

Recommendation 1

SSA should implement the HSPD-12 identity proofing, registration and issuance process nationwide for all new SSA employees and contractor personnel.

Comment

We partially agree with this recommendation for the study period. On December 15, 2005, the Office of Management and Budget (OMB) accepted SSA's HSPD-12 implementation plan template, which specified that the Agency would implement an HSPD-12 compliant personal identity verification system in phases, beginning with Headquarters employees and contractors. SSA is implementing that plan and has also begun the process to include employees who work in a field office (FO) facility where a badge is currently required.

Also, we began partially processing Agency new hires across the country under the Federal Information Processing Standards (FIPS) 201 guidelines. Specifically, we began conducting the Federal Bureau of Investigation (FBI) Criminal History Check (fingerprint check) before the new hires entered on duty (EOD) starting October, 2005, rather than after their EOD date. Previously, the FBI fingerprint check was not conducted until after the new hires EOD, which resulted in new hires being found to be unsuitable after EOD. The various regional servicing personnel offices also performed other checks based on guidance from SSA's Office of Personnel. Thus, SSA did take advantage of the new HSPD-12 process to screen new hires before bringing them on board. This part of our hiring process meets the directive.

We did not issue the building access badges according to the FIPS 201 separation-of-duties process in regional locations where such access badges are used. We did not attempt this, because we lacked the resources to train the regions and large sites on the process and to properly oversee implementation. It should be noted that most SSA FO employees do not receive building access badges. These badges are primarily issued in the larger SSA sites (e.g., regional offices, Program Service Centers, large Teleservice Centers and the Wilkes-Barre Data Operation Center). Since the vast majority of FO employees do not have badges, that part of FIPS 201 and OMB guidance did not apply to them for the study period.

October 2008 is our deadline for meeting this objective. We expect this deadline to be met.

Recommendation 2

SSA should ensure contract language is HSPD-12 compliant where appropriate.

Comment

We partially agree with this recommendation. During the study period, SSA did perform background checks on contractors, something not generally required for contractors prior to the signing of HSPD-12. We have performed such checks for about 20 years, putting us far ahead of most Federal agencies. SSA's Office of Acquisition and Grants already includes Federal Acquisition Regulation (FAR) 52.204-9, Personal Identity Verification of Contractor Personnel, in all applicable new contracts. During the study period, the General Services Administration (GSA) had not included language in the FAR to implement the requirements of HSPD-12. That FAR clause was not issued until after the study period. The Agency is working to revise the Security Requirements Clause to reflect that the new FAR language is in existing contracts.

Recommendation 3

SSA should issue credentials certified by GSA as having met Part 2 Personal Identity Verification *(PIV)* II credential technical requirements.

Comment

We agree with the recommendation, but we disagree with the rationale for making it based on the study period. We believe the problem with the initial testing of our credential was due to a flawed GSA testing process and not due to our card. The card we procured, and all the programs needed to issue the credentials stored in the card, came from the GSA Approved Products List. Thus, the cards should have worked as designed. We have resubmitted our credentials to GSA and expect that they will meet Part 2 PIV II technical requirements.

Recommendation 4

When available, implement the necessary infrastructure that will support and control the use of a compliant credential.

Comment

We agree. We have pilots underway and are actively pursuing the implementation of the required infrastructure. This process is expected to take at least 5 years and over $30 million to complete.

[In addition to the comments above, SSA provided technical comments which have been addressed in this report.]

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kitt Winter, Director, Data Analysis and Technology Audit Division, (410) 965-9702

Al Darago, Audit Manager, Application Controls, (410) 965-9710

Acknowledgments

In addition to those named above:

Harold Hunter, Auditor-in-Charge

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-14-07-27110

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.