



## SOCIAL SECURITY

### MEMORANDUM

Date: June 1, 2012

Refer To:

To: The Commissioner

From: Inspector General

Subject: Contractor Security of the Social Security Administration's Homeland Security Presidential Directive 12 Credentials (A-14-11-11106)

The attached final report presents the results of our review. Our objective was to assess the Social Security Administration's contractor process to safeguard Homeland Security Presidential Directive 12 credentials and the personally identifiable information contained on them.

Please provide within 60 days a corrective action plan that addresses each recommendation. If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

---

**OFFICE OF  
THE INSPECTOR GENERAL**

---

**SOCIAL SECURITY ADMINISTRATION**

---

**CONTRACTOR SECURITY  
OF THE SOCIAL SECURITY ADMINISTRATION'S  
HOMELAND SECURITY PRESIDENTIAL  
DIRECTIVE 12 CREDENTIALS**

**June 2012      A-14-11-11106**

---

**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: June 1, 2012

Refer To:

To: The Commissioner

From: Inspector General

Subject: Contractor Security of the Social Security Administration's Homeland Security Presidential Directive 12 Credentials (A-14-11-11106)

## OBJECTIVE

The objective of our review was to assess the Social Security Administration's (SSA) contractor process for safeguarding Homeland Security Presidential Directive 12 (HSPD-12)<sup>1</sup> credentials and the personally identifiable information (PII)<sup>2</sup> contained on them.

## BACKGROUND

HSPD-12 defines a common identification standard for Federal employees and contractors. HSPD-12 requires the development and implementation of a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal agencies to their employees and contractors so that they can gain physical access to federally controlled facilities or logical access to federally controlled information systems.<sup>3</sup>

OMB designated the General Services Administration (GSA) as the executive agent for the Government-wide acquisition of information technology products and services

---

<sup>1</sup> HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

<sup>2</sup> Office of Management and Budget (OMB) Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006, page 1, defines PII as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information that is linked or linkable to an individual.

<sup>3</sup> HSPD-12, *supra*.

required to implement HSPD-12.<sup>4</sup> When developing blanket purchase agreements for HSPD-12 products and service acquisitions, GSA is to ensure all approved suppliers provide products and services that meet all applicable Federal standards and requirements.<sup>5</sup> Federal agencies and departments are encouraged to use the acquisition services GSA provides.<sup>6</sup>

As the executive agent for HSPD-12 acquisitions, GSA develops a contractual relationship with the supplier. Federal agencies develop and send Statements of Work (SoW)<sup>7</sup> containing contract requirements to GSA. GSA uses the SoW as a contract to procure the products and services on behalf of the Federal agencies.

For instance, SSA worked with GSA to contract with a company that provided security and identity solutions and services based on smart card technologies to create the HSPD-12 credentials.<sup>8</sup> GSA served as SSA's contracting officer for the contract the Agency used to acquire the HSPD-12 credentials.<sup>9</sup>

SSA required that the contractor produce the smart cards for SSA's credentials and personalize the surface of the credential with the employee or contractor's full name and photograph, card's expiration date, card's identification number, and issuer's identification number.<sup>10</sup> The contractor created the credentials and delivered them to over 1,600 SSA locations nationwide. In the United States, the contractor has one facility to manufacture the credentials and another facility to personalize them. (See Appendix C for detailed description of the credential creation process.)

---

<sup>4</sup> OMB, M-05-24, *Implementation of HSPD-12 -- Policy for a Common Identification Standard for Federal Employees and Contractors*, Attachment A § 5.B, page 8 (August 5, 2005).

<sup>5</sup> Id.

<sup>6</sup> Id.

<sup>7</sup> SSA's Project Resource Guide glossary defines SoW as a document that outlines the specific supplies and services the project team wants delivered by a prospective contractor. The content of the SoW determines the type of contract that is awarded, influences the number and quality of proposals received, and serves as a baseline against which to evaluate proposals, and later, contractor performance.

<sup>8</sup> GSA Contract Number GS03T09DSC6003, Solicitation Number R3093975, (June 11, 2009).

<sup>9</sup> Id.

<sup>10</sup> *SoW*, *Social Security Administration, SSA PIV II Cards R3093975*, Section 2.3.3, page 3.

The *Federal Information Security Management Act of 2002* (FISMA) requires that each Federal agency provide information security protections for “(i) information collected or maintained by, or on behalf of, the agency and (ii) information systems used or operated by an agency or a contractor of an agency or other organization on behalf of an agency.”<sup>11</sup> Federal agencies must ensure their contractors comply with FISMA and related policy requirements<sup>12</sup> and include those requirements in contracts and grants.<sup>13</sup> In addition, HSPD-12 guidance<sup>14</sup> requires that Personal Identity Verification<sup>15</sup> (PIV) service providers use systems that are certified<sup>16</sup> according to Federal security standards, so all cards are issued by providers whose reliability has been appropriately accredited. Finally, OMB requires that agencies properly safeguard PII that is accessed remotely or physically transported outside an agency’s secured, physical perimeter.<sup>17</sup>

To achieve our objective, we reviewed the Agency’s contract and visited two contractor sites to view the contractor’s HSPD-12 credential production, personalization, and packaging and shipping processes.

---

<sup>11</sup> Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A), 44 U.S.C. § 3544(a)(1)(A). FISMA requires that the head of each agency be responsible for providing protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of such information and systems.

<sup>12</sup> According to OMB M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Frequently Asked Questions, Question 38, page 14 (September 14, 2011), Federal agencies must ensure their contractors abide by FISMA requirements.

<sup>13</sup> OMB, M-11-33, *supra*, Frequently Asked Questions, Question 41, page 17.

<sup>14</sup> According to Federal Information Processing Standards Publication (FIPS Pub.) 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006, Appendix B, Section B.2, p. 64, to accomplish the accreditation of PIV service providers and meet compliance with OMB Circular A-130, App. III, the Information Technology system(s) used by PIV service providers must be certified in accordance with NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

<sup>15</sup> NIST, SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, Executive Summary, page 1, (June 2008), states that PIV specifications are to be used as a foundation for securely identifying every individual seeking access to valuable and sensitive Federal resources, including buildings, information systems, and computer networks.

<sup>16</sup> NIST, SP 800-37 was revised to effectively include the certification and accreditation process as security authorization. See NIST, SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, pages B-1 and B-8 (February 2010).

<sup>17</sup> OMB, M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006).

## RESULTS OF REVIEW

Our interviews and observations found nothing to indicate the contractor's HSPD-12 credential manufacturing and personalization process had any physical and logical security control vulnerabilities<sup>18</sup> used to protect the HSPD-12 credentials and the PII contained in them. However, we did identify two contractor oversight concerns and two contract management issues that we want to bring to your attention.

- Contractor Oversight
  - SSA did not ensure the contractor personnel received appropriate training to safeguard Agency PII.
  - The contractor's information systems were not certified and accredited, as required by Federal guidance.
- Contract Management
  - SSA's GSA contract did not contain all the appropriate security clauses.
  - The contractor did not have a back-up facility in the United States, as required by the contract.

We discussed the contract management issues with SSA management and GSA's contracting officer. Based on our discussions, it is unclear which party is responsible for resolving these issues; therefore, we plan to submit our concerns to GSA's Office of Inspector General in a separate memorandum.

### **SSA DID NOT ENSURE CONTRACTOR PERSONNEL RECEIVED APPROPRIATE TRAINING TO SAFEGUARD AGENCY PII**

SSA did not ensure contractor personnel received appropriate training, such as user awareness training and training on safeguarding PII. During our review, we identified three contractor personnel who had regular access to SSA files that contained PII. When asked, contractor personnel could not identify specific policy or procedures that should be used in the event of a loss of PII.

Contractor personnel received security training when they are hired and annual refresher training. However, the majority of the training was on physical security controls, not PII protection. Although SSA established policies and procedures for PII protection, it did not ensure the contractor understood its responsibilities to safeguard PII. Without proper training on the Agency's policies and procedures, contractor personnel will not be aware of the expected responsibilities to protect PII, which unnecessarily places SSA's data at a higher risk of harm.

---

<sup>18</sup> The physical control is the implementation of security measures in a defined structure used to deter or prevent unauthorized access to sensitive material. Examples of physical controls are security guards, picture identification, and locked/dead-bolted doors. Logical controls are tools used for identification, authentication, authorization, and accountability in computer information systems.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed with relation to contractor services.<sup>19</sup> Agencies must ensure the contractor implements identical, not "equivalent," security procedures.<sup>20</sup> Furthermore, since SSA is a PIV card issuer,<sup>21</sup> it is responsible for the management and oversight of contractor services.<sup>22</sup> Specifically, the Agency is responsible for ensuring the contractor personnel receive appropriate training, such as user awareness training and training on agency policy and procedures.<sup>23</sup>

### **CONTRACTOR'S INFORMATION SYSTEMS WERE NOT CERTIFIED AND ACCREDITED, AS REQUIRED BY FEDERAL GUIDANCE**

SSA did not perform a certification and accreditation (C&A)<sup>24,25</sup> review of the contractor's information systems or obtain assurance from GSA or the contractor that an appropriate C&A had been performed, as required by NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*,<sup>26</sup> and FIPS Pub. 201-1, *Personal Identity Verification of Federal Employees and Contractors*.<sup>27</sup>

Agency officials stated that GSA, as the executive agent appointed by OMB, provided a certified list of vendors that met all Federal requirements. SSA has accepted this certification and believes that the vendor has met all the needed FISMA requirements.

It was not apparent that the GSA certification also incorporated FISMA requirements. To that end, we asked GSA whether it had performed a C&A review on the contractor's systems as well as requested any related C&A documentation. To date, GSA has not provided us any of the requested information.

---

<sup>19</sup> OMB, M-11-33, *supra*, Frequently Asked Questions, Question 40, pages 15 and 16.

<sup>20</sup> *Id.*

<sup>21</sup> According to NIST, SP 800-79-1, *supra* at page 8, PIV Card Issuer includes all functions required to produce, issue, and maintain PIV Cards for an organization.

<sup>22</sup> NIST, SP 800-79-1, *supra* at §2.1, page 8.

<sup>23</sup> OMB, M-11-33, *supra*, Frequently Asked Questions, Question 40, pages 15 and 16.

<sup>24</sup> FIPS, Pub. 201-1, *supra*, at Appendix B, Section B.2, page 64.

<sup>25</sup> NIST, SP 800-37, Revision 1, *supra* at pp. B-1 and B-8, defines the security authorization as "The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls."

<sup>26</sup> NIST SP 800-79-1 states PIV Card Issuer information systems are certified in accordance with NIST SP 800-37, Appendix G, page 66.

<sup>27</sup> FIPS, Pub. 201-1, *supra*, at Appendix B, section B.2, page 64. Also, see Footnote 13.



FISMA requires that agencies ensure contractors handling Federal information or operating information systems on the Government's behalf meet the same security requirements as Federal agencies.<sup>28</sup> OMB requires that agencies obtain sufficient assurance that security controls over contractor systems are effectively implemented and comply with Federal and agency guidelines.<sup>29</sup>

The Agency is responsible for ensuring the contractor's information systems meet Federal security requirements. Therefore, SSA should have obtained evidence of a proper C&A review from GSA or the contractor.

As a result of SSA not obtaining the aforementioned evidence, the Agency may not have been fully aware of the contractor's risks and whether effective security controls were implemented at the contractor's facility. During our discussions with the contractor personnel, they stated the company had conducted periodic security reviews to meet other client's security requirements.

We requested the contractor provide security requirements it deploys when providing similar services to other clients. Our goal was to compare those requirements to Federal security standards; however, the contractor could not provide this documentation because of non-disclosure agreements with other clients. Instead, the contractor provided documentation that demonstrated how it met the clients' security requirements for the past 2 years. Although it appears the contractor met its other clients' security requirements, we were unable to determine whether the security measures deployed by the contractor met Federal security standards. It should be noted that the contractor's services to other clients involve sensitive personal information similar to that of SSA.

We recommend SSA request documentation from GSA that the contractor's information systems are certified and accredited as required by Federal requirements. However, if GSA did not perform a C&A review of the contractor's information systems, SSA should seek guidance from OMB to determine which agency is responsible for conducting this review of the contractor's information systems.

---

<sup>28</sup> Pub. L. No. 107-347, Title III, Section 301 §3544(a)(1)(A)(ii). Also, see OMB, M-11-33, *supra*, Frequently Asked Questions, Question 40, page 16.

<sup>29</sup> Department of Homeland Security (DHS), *FY 2011 Inspector General Federal Information Security Management Act Reporting*, Version 1.0, question 10.a(2) (June 1, 2011). In July 2010, DHS began exercising primary responsibility within the executive branch for the operational aspects of Federal cybersecurity with respect to the Federal information systems that fall within FISMA under 44 U.S.C. § 3543. DHS provided Fiscal Year (FY) 2011 FISMA reporting instructions to Federal Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy. OMB, M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*, pages 1 and 2, July 6, 2010. Also, see M-11-33, *supra*, page 1.


## CONCLUSION AND RECOMMENDATIONS

Based on our interviews and observations, nothing came to our attention that indicated the contractor's card manufacturing and personalization process had any vulnerability in its physical and logical security controls used to protect the HSPD-12 credentials and the PII contained on them. However, we did identify some management oversight concerns that we wanted to bring to your attention to help ensure the continued security of the Agency's HSPD-12 credentials. Because of these concerns, we recommend SSA:

1. Ensure contractor personnel receive appropriate training on Agency's policies and procedures for safeguarding PII.
2. Request documentation from GSA that the contractor's information systems are certified and accredited as required by Federal requirements. However, if GSA did not perform a C&A review of the contractor's information systems, SSA should seek guidance from OMB to determine which agency is responsible for conducting this review on the contractor's information systems.

## AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with our recommendations. See Appendix D for the Agency's comments.



Patrick P. O'Carroll, Jr.

# *Appendices*

---

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Homeland Security Presidential Directive 12 Creation Process

APPENDIX D – Agency Comments

APPENDIX E – OIG Contacts and Staff Acknowledgments

## Acronyms

C&A	Certification and Accreditation
DHS	Department of Homeland Security
FIPS PUB.	Federal Information Processing Standards Publication
FISMA	<i>Federal Information Security Management Act of 2002</i>
FY	Fiscal Year
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
Pub. L. No.	Public Law Number
SoW	Statement of Work
SP	Special Publication
SSA	Social Security Administration
U.S.C.	United States Code

# Scope and Methodology

To meet the objectives of our review, we performed the following procedures.

1. Reviewed the General Service Administration's contract document (Contract Number GS03T09DSC6003), *Statement of Work, Social Security Administration, SSA PIV II Cards, R3093975* to determine whether the Social Security Administration (SSA) included all appropriate security and contract clauses in the contract.
2. Observed SSA's process for transferring Agency employee and contractor personally identifiable information (PII)<sup>1</sup> to the contractor's system to determine whether the transfer complied with SSA and Federal requirements.
3. Conducted on-site visits of the contractor's Homeland Security Presidential Directive 12 (HSPD-12) credentials production, personalization, and packaging and shipping processes at two contractor sites. We observed the creation of the HSPD-12 credentials and observed the contractor's physical and logical security controls implemented to protect SSA's credentials. We visited two of the contractor's facilities: the manufacturing site and the personalization facility in the United States. No testing of the contractor's physical and logical security controls was performed.
4. Compared and assessed the contractor's process to safeguard PII to relevant Federal laws, regulations, standards, and guidelines.

We also reviewed the following.

- *The Privacy Act of 1974*, as amended, 5 U.S.C. 552a;
- *The Federal Information Security Management Act of 2002*; 44 U.S.C. 3541 et seq.;
- Office Management and Budget (OMB) Memorandum M-05-24, *Implementation of HSPD-12--Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005; Attachment B HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004;
- OMB, M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 14, 2011;

---

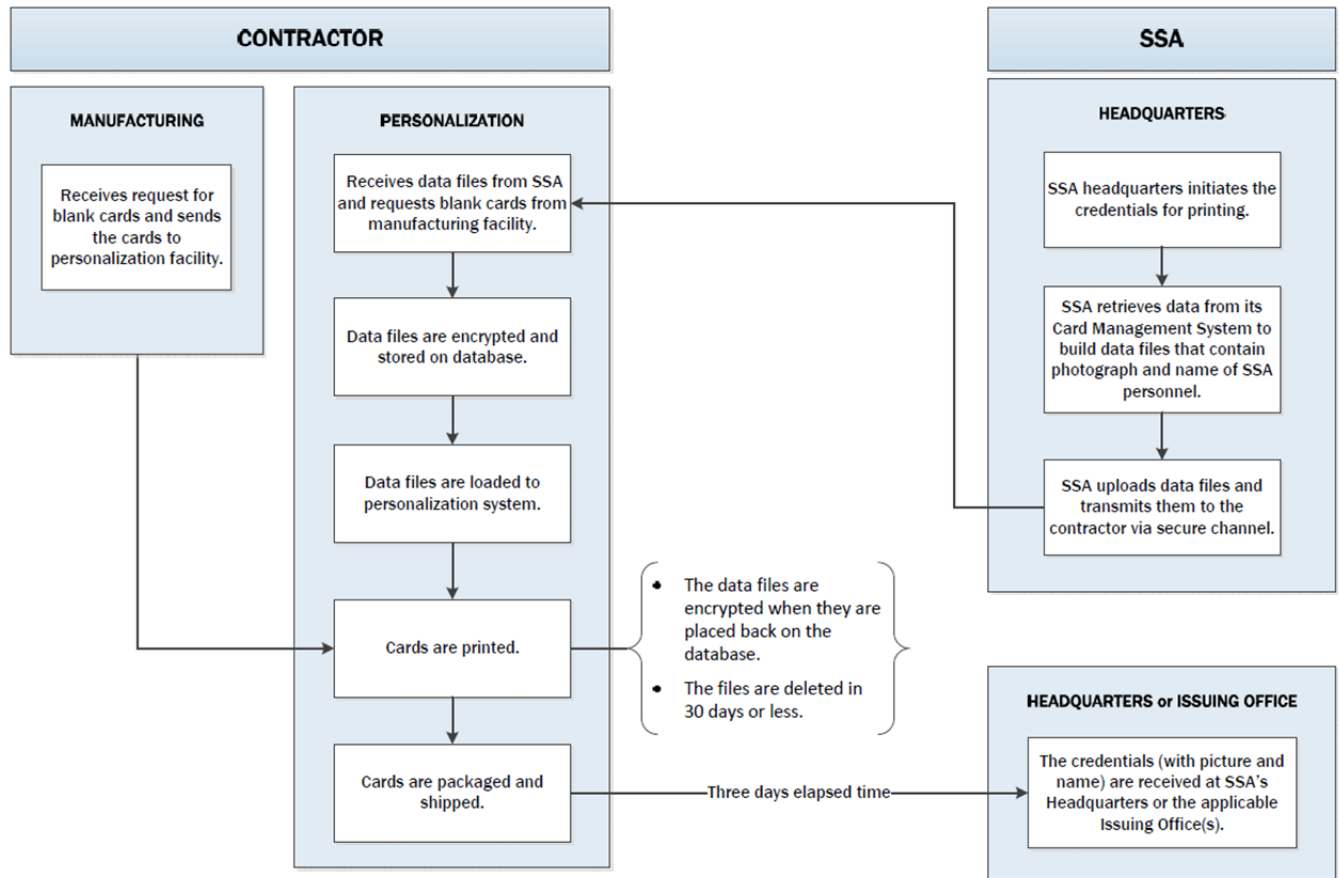
<sup>1</sup> OMB, Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006, page 1, defines PII as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

- OMB, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007;
- OMB, M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006;
- OMB, M-03-22, *Office of Management and Budget Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003;
- General Services Administration Federal Supply Service Memorandum, *Acquisition of Products and Services for Implementation of HSPD-12*, August 10, 2005;
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, February 8, 1996;
- Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006;
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls of Federal Information Systems and Organizations*, August 2009;
- NIST, SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008;
- NIST, SP 800-122, *Guide to Protecting the Confidentiality of PII*, April 2010; and
- NIST, SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.

We performed our fieldwork at SSA's contractor facilities and Headquarters from June through September 2011. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## Homeland Security Presidential Directive -12 Creation Process

As part of the credential creation process, the Social Security Administration (SSA) electronically transmits data files<sup>1</sup> containing personally identifiable information to the contractor. The data files are transmitted through an encrypted channel.<sup>2</sup> Once the contractor receives the data files, the pre-manufactured credential is personalized. In turn, the contractor ships the credentials via Federal Express to SSA. Once received, SSA adds additional information<sup>3</sup> to the credential before issuing it to the appropriate employee or contractor. See the diagram below.



<sup>1</sup> The files contain SSA employee or contractor's first name, middle initial, last name, card expiration date, agency affiliation, and photograph.

<sup>2</sup> SSA used Secure Shell to interact with the contractor's card production system. Secure Shell provides a secure data communication between two networked computers that connects through a secure channel.

<sup>3</sup> SSA downloads electronic certificates for authentication purposes onto the credentials.

## Agency Comments





## SOCIAL SECURITY

### MEMORANDUM

**Date:** May 24, 2012 **Refer To:** S1J-3

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

**From:** Dean S. Landis /s/  
Deputy Chief of Staff

**Subject:** Office of the Inspector General Draft Report, "Contractor Security of the Social Security Administration's Homeland Security Presidential Directive 12 Credentials"  
(A-14-11-11106)—INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Amy Thompson at (410) 966-0569.

Attachment

**COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT,  
“CONTRACTOR SECURITY OF THE SOCIAL SECURITY ADMINISTRATION’S  
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 CREDENTIALS”  
(A-14-11-11106)**

**Recommendation 1**

Ensure contractor personnel receive appropriate training on Agency’s policies and procedures for safeguarding PII.

**Response**

We agree. We will provide the contractor with appropriate policies and training materials on safeguarding personally identifiable information.

**Recommendation 2**

Request documentation from GSA that the contractor’s information systems are certified and accredited as required by Federal requirements. However, if GSA did not perform a C & A review of the contractor’s information systems, SSA should seek guidance from OMB to determine which agency is responsible for conducting this review on the contractor’s information systems.

**Response**

We agree.

## OIG Contacts and Staff Acknowledgments

### ***OIG Contacts***

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Audit Manager

### ***Acknowledgments***

In addition to those named above:

Tina Nevels, Auditor

For additional copies of this report, please visit our Website at <http://oig.ssa.gov/> or contact the Office of the Inspector General's Public Affairs Staff at (410) 965-4518. Refer to Common Identification Number A-14-11-11106.

## ***DISTRIBUTION SCHEDULE***

Commissioner of Social Security

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, Committee on the Budget, House of Representatives

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

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 Pensions 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 an Office of Audit (OA), Office of Investigations (OI), Office of the Counsel to the Inspector General (OCIG), Office of External Relations (OER), and Office of Technology and Resource Management (OTRM). To ensure compliance with policies and procedures, internal controls, and professional standards, the OIG also has a comprehensive Professional Responsibility and Quality Assurance program.

### **Office of Audit**

OA conducts 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 reviews and program evaluations on issues of concern to SSA, Congress, and the general public.

### **Office of Investigations**

OI conducts investigations 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 liaison to the Department of Justice on all matters relating to the investigation of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

### **Office of the Counsel to the Inspector General**

OCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCIG 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. Also, OCIG administers the Civil Monetary Penalty program.

### **Office of External Relations**

OER manages OIG's external and public affairs programs, and serves as the principal advisor on news releases and in providing information to the various news reporting services. OER develops OIG's media and public information policies, directs OIG's external and public affairs programs, and serves as the primary contact for those seeking information about OIG. OER prepares OIG publications, speeches, and presentations to internal and external organizations, and responds to Congressional correspondence.

### **Office of Technology and Resource Management**

OTRM supports OIG by providing information management and systems security. OTRM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, OTRM is the focal point for OIG's strategic planning function, and the development and monitoring of performance measures. In addition, OTRM receives and assigns for action allegations of criminal and administrative violations of Social Security laws, identifies fugitives receiving benefit payments from SSA, and provides technological assistance to investigations.