SOCIAL SECURITY
Office of the Commissioner

November 15, 2011

The Honorable Jacob J. Lew
Director, Office Management and Budget
Eisenhower Executive Office Building
Washington, D.C. 20505

Dear Mr. Lew,

As required by the Office of Management and Budget's (OMB) Memorandum 11-33 (M-11-33), *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, we are submitting our Fiscal Year 2011 Information Technology Security Program Review Report using the CyberScope tool. Our submission includes our responses to the reporting questions as well as the reports of our Senior Agency Official for Privacy and our Office of the Inspector General (OIG). OIG's report includes an independent evaluation of our information security program and FISMA compliance.

Additionally, M-11-33 instructs agencies to submit their current documentation related to OMB Memorandum 07-16 (M-07-16), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* Accordingly, we are submitting the following information per M-07-16:

- Implementation plan and progress update on eliminating unnecessary use of Social Security Numbers; and
- Implementation plan and progress update on review and reduction of holdings of personally identifiable information.

Our FISMA report substantially agrees with our Inspector General's FISMA report. We will continue to enhance our overall security posture. If you have any questions about this information, please contact me, or have your staff contact our Chief Information Officer, Kelly Croft, at (410) 965-7481, or by email at Kelly.Croft@ssa.gov.

Sincerely,

Michael J. Astrue

SOCIAL SECURITY
Office of the Commissioner

November 15, 2011

The Honorable Jacob J. Lew
Director, Office Management and Budget
Eisenhower Executive Office Building
Washington, D.C. 20505

Dear Mr. Lew,

As required by the Office of Management and Budget's (OMB) Memorandum 11-33 (M-11-33), *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, we are submitting our Fiscal Year 2011 Information Technology Security Program Review Report using the CyberScope tool. Our submission includes our responses to the reporting questions as well as the reports of our Senior Agency Official for Privacy and our Office of the Inspector General (OIG). OIG's report includes an independent evaluation of our information security program and FISMA compliance.

Additionally, M-11-33 instructs agencies to submit their current documentation related to OMB Memorandum 07-16 (M-07-16), *Safeguarding Against and Responding to the Breach of Personally Identifiable Information.* Accordingly, we are submitting the following information per M-07-16:

- Implementation plan and progress update on eliminating unnecessary use of Social Security Numbers; and
- Implementation plan and progress update on review and reduction of holdings of personally identifiable information.

Our FISMA report substantially agrees with our Inspector General's FISMA report. We will continue to enhance our overall security posture. If you have any questions about this information, please contact me, or have your staff contact our Chief Information Officer, Kelly Croft, at (410) 965-7481, or by email at Kelly.Croft@ssa.gov.

Sincerely,

Michael J. Astrue

Chief Information Officer

Section Report

2011

Annual FISMA Report

Social Security Administration

Section 1: System Inventory

1. For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Agency operational, FISMA reportable, systems by Agency component (i.e. Bureau or Sub-Department Operating Element).

Agency/ Component		1a. Agency Operated Systems	1b. Contractor Operated Systems on Behalf of the Agency.	Total Systems	1c. Number of systems in 1a. and 1b. combined with security authorization to operate.	1d. Systems or Services leveraging a public cloud.	1e. Number of Systems and Services in 1d. with a Security Assessment and Authorization to utilize.
SSA	High	0	0	0	0	0	0
	Moderate	16	0	16	16	0	0
	Low	5	0	5	5	0	0
	Not Categorized	0	0	0	0	0	0
	Sub-Total	***21***	***0***	***21***	***21***	0	0
	The SSA inventory process accounts for contractor systems by incorporating them into larger system authorization boundaries. These contractor components are documented accordingly in the applicable System Security Plans (SSP).						
Agency Totals	High	0	0	0	0	0	0
	Moderate	16	0	16	16	0	0
	Low	5	0	5	5	0	0
	Not Categorized	0	0	0	0	0	0
	Sub-Total	***21***	***0***	***21***	***21***	0	0

Section 2: Asset Management

2.1 Provide the total number of Agency Information Technology assets (e.g. router, server, workstation, laptop, Blackberry, etc.)

249215

2.1a. Provide the number of Agency information technology assets, connected to the network, (e.g. router, server, workstation, laptop, etc.) where an automated capability provides visibility at the Agency level into asset inventory information.

215396

2.1b. Provide the number of Agency information technology assets where an automated capability produces Security Content Automation Protocol (SCAP) compliant asset inventory information output.

174018

2.1c. Provide the number of Agency information technology assets where all of the following asset inventory information is collected: Network address, Machine Name, Operating System, and Operating System/Patch Level.

200186

2.2 Has the Agency implemented an automated capability to detect and block unauthorized software from executing on the network?

Partial Coverage

2.3 Has the Agency implemented an automated capability to detect and block unauthorized hardware from connecting to the network?

Partial Coverage

2.4 For your Agency, which type(s) of assets are the most challenging in performing automated asset management? Rank the asset types below from 1-4 with 1 being the most challenging.

2.4a. Servers

3

2.4b. Workstations/Laptops

2

2.4c. Network Devices

4

Section 2: Asset Management

2.4d. Mobile Devices

1

Section 3: Configuration Management

3.1 Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into system configuration information (e.g. comparison of Agency baselines to to installed configurations).

178999

3.1a. Provide the number of Agency information technology assets where an automated capability produces SCAP compliant system configuration information output.

174018

3.2 Provide the number of types of operating system software in use across the Agency

11

Comments:

SSA uses the following operating systems:

Windows 2000 Server
Windows 2003 Server
Windows 2008 Server
Windows Vista
Windows 7
Solaris
Aix
HP-UX
AS400/iSeries
Cisco IOS
Linux

3.2a. Provide the number of operating system software in use across the Agency for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security baseline.

10

Section 3: Configuration Management

3.3 Provide the number of enterprise-wide applications (e.g. Internet Explorer, Adobe, MS Office, Oracle, SQL, etc.) in use at the Agency.

19

3.3a. Provide the number of enterprise-wide applications for which standard security configuration baselines are defined. Consider an Agency approved deviation as part of the Agency standard security configuration baseline.

5

Section 4: Vulnerability Management

4.1 Provide the number of Agency information technology assets where an automated capability provides visibility at the Agency level into detailed vulnerability information (Common Vulnerabilities and Exposures - CVE)

178999

4.1a. Provide the number of Agency information technology assets where an automated capability produces SCAP compliant vulnerability information output.

174018

Section 5: Identity and Asset Management

5.1 What is the number of Agency network user accounts (Exclude system and application accounts utilized by processes)?

93717

5.1a. How many network user accounts are configured to require PIV to authenticate to the Agency network(s)?

0

5.1b. How many network user accounts are configured to optionally use PIV to authenticate to the Agency network(s)?

93717

5.2 What is the number of Agency privileged network user accounts (e.g. system administrators)?

7020

5.2a. What is the number of Agency privileged network user accounts that are configured to require PIV credentials to authenticate to Agency network(s)?

0

5.2b. What is the number of Agency privileged network user accounts that are configured to optionally use PIV credentials to authenticate to the Agency network(s)?

7020

Section 6: Data Protection

6.1 Provide the total number of:

6.1a. Mobile computers and devices (excluding laptops)

6.1a(1) Netbooks

831

6.1a(2) Tablet-type computers

671

6.1a(3) Blackberries

4139

6.1a(4) Smartphones

0

6.1a(5) USB devices (Flash drives and external hard drives)

0

Comments: SSA does not track this information at this time; however, the agency has employed controls that ensure any data stored on these devices is encrypted per US Government standards.

6.1a(6). Other

0

6.1b. Laptops Only

11813

6.2 Provide the number of devices in 6.1 that have all user data encrypted with FIPS 140-2 validated encryption.

6.2a. Mobile computers and devices (excluding laptops)

6.2a(1). Netbooks

831

6.2a(2) Tablet-type computers

671

6.2a(3). Blackberries

4139

Section 6: Data Protection

6.2a(4) Smartphones

0

6.2a(5) USB devices (Flash drives and external hard drives)

0

Comments: SSA does not track this information at this time; however, the agency has employed controls that ensure any data stored on these devices is encrypted per US Government standards.

6.2a(6) Other

0

6.2b. Laptops only

11813

6.3 Provide the percentage of Agency email systems that implement encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public such as S/MIME, PGP, or other.

100%

Section 7: Boundary Protection

7.1 Provide the percentage of the required TIC 1.0 capabilities that are implemented. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

96%

7.1a Provide the percentage of TIC 2.0 Capabilities that are implemented. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

94%

7.2 Provide the percentage of TICS with operational NCPS (Einstein 2) deployment. (Applies only to Federal Civilian Agency TIC Access Providers (TICAP) only. All others should respond N/A.)

100%

7.3 Provide the percentage of external network capacity passing through a TIC/MTIPS. (Applies to all Federal Civilian Agencies. DOD should respond N/A.)

100%

Section 7: Boundary Protection

7.4 Provide the percentage of external connections passing through a TIC/MTIPS. (Applies to all Federal Civilian Agencies. DOD should respond N/A.)

100%

7.5 Provide the percentage of Agency email systems that implement sender verification (anti-spoofing) technologies when sending messages to government agencies or the public such as DKIM, SPF, or other.

100%

7.6 Provide the percentage of Agency email systems that check sender verification (anti-spoofing technologies) to detect possibly forged messages from government agencies known to send email with sender verification such as DKIM or SPF or other.

100%

7.7 Provide the frequency with which the Agency conducts thorough scans for unauthorized wireless access points.

Daily

7.8 Provide the frequency in which the Agency maps their cyber perimeter (e.g. externally visible systems and devices).

Monthly

Section 8: Incident Management

8.1 What is the number of Agency operational networks on which controlled network penetration testing was performed in the past year?

1

For the testing conducted above, provide the following information:

8.1a. Percentage of incidents detected by NOC/SOC. (Per NIST 800-61, an incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.)

90%

For the incidents above detected by NOC/SOC during penetration testing provide the following information:

8.1a(1) Mean-time to incident detection, in hours. (The mean time-to-incident detection metric is calculated by subtracting the Date of Occurrence from the Date of Discovery. These metrics are then averaged across the number of incidents detected by the NOC/SOC during penetration testing.)

0 hours 0 minutes

Comments: It is not possible to answer this question based on current capabilities.

Section 8: Incident Management

8.1a(2) Mean-time to incident remediation, in hours. (The mean time-to-incident remediation is calculated by dividing the difference between the Date of Occurrence and the Date of Remediation for each incident remediated in the metric time period, by the total number of incidents remediated in the metric time period.)

94 hours 0 minutes

8.1a(3) Mean-time to incident recovery, in hours. (The mean time-to-incident recovery is calculated by dividing the difference between the Date of Occurrence and the Date of Recovery for each incident recovered in the metric time period, by the total number of incidents recovered in the metric time period.)

94 hours 0 minutes

8.1b. Percentage of penetration testing incidents detected from other sources or business processes.

0%

8.2 For FY11, what percentage of applicable US-CERT SARs (Security Awareness Report or Information Assurance Vulnerability Alerts for DOD) has been acted upon appropriately by the Agency?

100%

8.3 Provide the number of times in the past year the Agency participated in the Joint Agency Cyber Knowledge Exchange (JACKE). (These meetings are monthly) (DOD should respond N/A.)

9

Section 9: Training and Education

9.1 What is the average frequency with which users receive supplemental cybersecurity awareness training content beyond the annual training requirement (content could include a single question or tip of the day)?

Bureau	Frequency with which users receive supplemental cybersecurity awareness training
SSA	Quarterly

9.2 Provide the total number of Agency sponsored phishing attack exercises, if conducted.

0

9.2a. Provide the number of Agency sponsored phishing attack exercises that revealed results of potential compromise (e.g., users clicked on an embedded link).

0

Section 9: Training and Education

9.3 Provide the number of Agency users with network access privleges.

93717

9.3a. Provide the number of Agency users with network access privileges that have been given security awareness training annually.

93717

9.4 Provide the number of Agency network users with significant security responsibilities.

367

9.4a. Provide the number of Agency network users with significant security responsibilities that have been given specialized, role based, security training annually.

367

9.5 At what frequency is security awareness training content (that is provided to users) updated by the Agency or training provider?

Monthly

9.5a Comments:

N/A

9.6 At what frequency is specialized, role based, security training content (that is provided to users) updated by the Agency or training provider?

Annual

9.6a. Comments:

N/A

9.7 Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access.

100%

9.8 Does your Agency's annual security awareness training include:

9.8a. Information on the security risks of wireless technologies and mobile devices?

Yes

9.8b. Awareness of the organization's security policies/procedures for mobile devices?

Yes

Section 9: Training and Education

9.8c. Mitigation of risks by maintaining physical control of mobile devices, encrypting sensitive information, disabling wireless functionality when not in use, and procedures for reporting lost or stolen mobile devices?

Yes

9.8d. Content on how to recognize and avoid phishing attacks?

Yes

Section 10: Remote Access

10.1 Provide the number of remote access connection methods (e.g. Dial-up, VPN, Clientless-VPN or SSL, etc.) the Agency offers to allow users to connect remotely to full access of normal desktop Agency LAN/WAN resources/services. Connection methods refer to options the Agency offers to users allowing them to connect remotely.

1

10.1a. For those methods provided above, provide the number that:

10.1a(1) Require only UserID/password.

0

10.1a(2) Require only PIV credentials.

0

10.1a(3) Optionally accepts PIV credentials.

0

10.1a(4) Require other forms of two-factor authentication.

1

10.1a(5) Utilize FIPS 140-2 validated cryptographic modules.

1

10.1a(6) Prohibit tunneling and/or dual connected laptops where the laptop has both an active wired and wireless connection.

1

10.1a(7) Are configured, in accordance with OMB M-07-17, to time-out after 30 minutes of inactivity which requiring re-authentication.

1

Section 10: Remote Access

10.1a(8) Scan for malware upon connection.

0

Comments: The Cisco VPN employs a Network Access Control (NAC) base solution that performs compliance checks to ensure that remote computers connecting to SSANET via VPN adhere to SSA's software standards. Specifically, NAC enforces compliance with up to date Virus Signatures, Hard Disk encryption for laptops, and a functioning Microsoft System Center Configuration Manager (SCCM) client to ensure timely updates and patches. The anti-virus client periodically scans the local hosts.

10.1a(9) Require Government Furnished Equipment (GFE).

1

10.1b. For those connection methods that require GFE as in question 10.1a(9) above, provide the number of connection methods that:

10.1b(1) Assess and correct system configuration upon connection.

1

10.2 List the remote access connection methods identified in 10.1:

Remote access connection method
CISCO VPN w/PIV compliant authentication

Section 11: Network Security Protocols

11.1 Provide the number of:

11.1a. External facing DNS names (second-level, e.g. www.dhs.gov).

8

11.1b External facing DNS names (second-level) signed.

4

11.1c Provide the percentage of external facing DNS hierarchies with all sub-domains (second-level and below) entirely signed.

100%

Section 12: Software Assurance

Section 12: Software Assurance

12.1 Provide the number of information systems, developed in-house or with commercial services, deployed in the past twelve months.

49

12.1a. Provide the number of information systems above (12.1) that were tested using automated source code testing tools. (Source code testing tools are defined as tools that review source code line by line to detect security vulnerabilities and provide guidance on how to correct problems identified.)

0

12.1b. Provide the number of the information systems above (12.1a) where the tools generated output is compliant with:

12.1b(1) Common Vulnerabilities and Exposures (CVE)

0

12.1b(2) Common Weakness Enumeration (CWE)

0

12.1b(3) Common Vulnerability Scoring System (CVSS)

0

12.1b(4) Open Vulnerability and Assessment Language (OVAL).

0

Section 13: Continuous Monitoring

13.1 What percentage of data from the following potential data feeds are being monitored at appropriate frequencies and levels in the Agency:

13.1a IDS/IPS

100%

13.1b AV/Anti-Malware/Anti-Spyware

100%

13.1c System Logs

0%

13.1d Application Logs

0%

Section 13: Continuous Monitoring

13.1e Patch Status

80%

13.1f Vulnerability Scans

100%

13.1g DNS logging

0%

13.1h Configuration/Change Management system alerts

0%

13.1i Failed logins for privileged accounts

100%

13.1j Physical security logs for access to restricted areas (e.g. data centers)

100%

13.1k Data loss prevention data

100%

13.1l Remote access logs

0%

13.1m Network device logs

0%

13.1n Account monitoring

100%

13.1n(1) Locked out

100%

13.1n(2) Disabled

100%

13.1n(3) Terminated personnel

100%

Section 13: Continuous Monitoring

13.1n(4) Transferred personnel

100%

13.1n(5) Dormant accounts

100%

13.1n(6) Passwords that have reached the maximum password age

100%

13.1n(7) Passwords that never expire

100%

13.1o Outbound traffic to include transfers of data, either encrypted or unencrypted.

50%

13.1p Port scans

0%

13.1q Network access control lists and firewall rules sets.

100%

13.2 To what extent is the data collected, correlated, and being used to drive action to reduce risks? Please provide a number on a scale of 1-5, with 1 being that "All continuous monitoring data is correlated"

3

Inspector General

Section Report

2011

Annual FISMA Report

Social Security Administration

Section 1: Risk Management

1a. **The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

1.a(1). **Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.**

Yes

1.a(2). **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1**

Yes

1.a(3). **Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.**

Yes

1.a(4). **Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.**

Yes

1.a(5). **Categorizes information systems in accordance with government policies.**

Yes

1.a(6). **Selects an appropriately tailored set of baseline security controls.**

Yes

1.a(7). **Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

Yes

Comments: Due to budget cuts, the Social Security Administration (SSA) stated that it did not update the System Security Plans for two of its general support systems and did not perform annual security tests on them.

1.a(8). **Assesses the security controls using appropriate assessment procedures 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.**

Yes

Section 1: Risk Management

1.a(9). **Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.**

Yes

1.a(10). **Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.**

Yes

1.a(11). **Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.**

Yes

1.a(12). **Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).**

Yes

1.a(13). **Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.**

Yes

1.a(14). **Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.**

Yes

Section 2: Configuration Management

2.a. **The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:**

2.a(1). **Documented policies and procedures for configuration management.**

Yes

2.a(2). **Standard baseline configurations defined.**

Section 2: Configuration Management

Yes

Comments: The Agency has established baseline configurations for most, but not all environments. SSA does not have configuration baselines for two systems.

2.a(3). Assessing for compliance with baseline configurations.

Yes

Comments: We identified some weaknesses with SSA's monitoring of configuration settings.

2.a(4). Process for timely, as specified in Agency policy or standards, remediation of scan result deviations.

Yes

2.a(5). For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

Yes

2.a(6). Documented proposed or actual changes to hardware and software configurations.

Yes

2.a(7). Process for timely and secure installation of software patches.

Yes

Section 3: Incident Response and Reporting

3a. The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

3a(1). Documented policies and procedures for detecting, responding to and reporting incidents.

Yes

Comments: SSA can improve its incident response and reporting program by establishing additional guidance on reporting incidents to the Office of the Inspector General (OIG) and law enforcement.

3a(2). Comprehensive analysis, validation and documentation of incidents.

Yes

3a(3). When applicable, reports to US-CERT within established timeframes.

Section 3: Incident Response and Reporting

Yes

3a(4). When applicable, reports to law enforcement within established timeframes.

No

Comments: SSA does not have an established timeframe for reporting incidents to law enforcement or the OIG. Additionally, SSA did not report any PII incidents to OIG due to an incorrect email address in its system.

3a(5). Responds to and resolves incidents in a timely manner, as specified in Agency policy or standards, to minimize further damage.

Yes

Comments: SSA reports security incidents to the United States Computer Emergency Readiness Team timely. However, SSA has not established a timeframe to report security related incidents to law enforcement and the OIG. In addition, OIG did not receive any referrals for further investigation.

3a(6). Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

Comments: SSA does not use virtual/cloud environments.

3a(7). Is capable of correlating incidents.

Yes

Section 4: Security Training

4.a. The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

4.a(1). Documented policies and procedures for security awareness training.

Yes

4.a(2). Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

4.a(3). Security training content based on the organization and roles, as specified in Agency policy or standards.

Yes

Section 4: Security Training

4.a(4). Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training.

No

Comments: SSA currently does not track security awareness training for contractors. SSA stated it would have an automated system to track security awareness training next fiscal year.

4.a(5). Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Agency users) with significant information security responsibilities that require specialized training.

No

Comments: SSA was not able to provide a comprehensive list of contractors with significant information security responsibilities. Therefore, we were unable to test this area.

Section 5: POA&M

5.a. The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

5.a(1). Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

Yes

5.a(2). Tracks, prioritizes and remediates weaknesses.

Yes

5.a(3). Ensures remediation plans are effective for correcting weaknesses.

Yes

5.a(4). Establishes and adheres to milestone remediation dates.

Yes

5.a(5). Ensures resources are provided for correcting weaknesses.

Yes

5.a(6). Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Section 5: POA&M

Yes

Section 6: Remote Access Management

6.a. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

6.a(1). Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

6.a(2). Protects against unauthorized connections or subversion of authorized connections.

Yes

6.a(3). Users are uniquely identified and authenticated for all access.

Yes

6.a(4). If applicable, multi-factor authentication is required for remote access.

Yes

6.a(5). Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

6.a(6). Defines and implements encryption requirements for information transmitted across public networks.

Yes

6.a(7). Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.

Yes

Section 7: Identity and Access Management

7.a. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

7.a(1). Documented policies and procedures for account and identity management.

Section 7: Identity and Access Management

Yes

7.a(2). Identifies all users, including federal employees, contractors, and others who access Agency systems.

Yes

7.a(3). Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

7.a(4). If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.

Yes

7.a(5). Ensures that the users are granted access based on needs and separation of duties principles.

Yes

Comments: We identified some weaknesses with SSA's process to ensure that users are granted access based on need and the separation of duties principles.

7.a(6). Identifies devices that are attached to the network and distinguishes these devices from users.

Yes

Comments: We identified some weaknesses with SSA's process to identify devices attached to its network.

7.a(7). Ensures that accounts are terminated or deactivated once access is no longer required.

Yes

Comments: We identified some weaknesses with SSA's process to ensure that accounts are terminated or deactivated once access is no longer required.

7.a(8). Identifies and controls use of shared accounts.

Yes

Comments: SSA stated that it does not allow users to share accounts.

Section 8: Continuous Monitoring Management

8.a. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

Section 8: Continuous Monitoring Management

8.a(1). Documented policies and procedures for continuous monitoring.

Yes

8.a(2). Documented strategy and plans for continuous monitoring.

Yes

8.a(3). Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.

Yes

Comments: SSA has not implemented configuration monitoring tools for some of its servers.

8.a(4). Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.

Yes

Comments: There are Continuous Monitoring data not readily accessible to SSA's Chief Information Security Officer.

Section 9: Contingency Planning

9.a. The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

9.a(1). Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

Yes

9.a(2). The Agency has performed an overall Business Impact Analysis (BIA).

Yes

Comments: SSA's last Business Impact Analysis was conducted in 2004.

9.a(3). Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

Comments: The contingency plan for one system has remained in draft form since Fiscal Year 2008.

Section 9: Contingency Planning

9.a(4). Testing of system specific contingency plans.

Yes

Comments: SSA's disaster recovery exercise included 19 of the Agency's 21 major systems and applications.

9.a(5). The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.a(6). Development of test, training, and exercise (TT&E) programs.

Yes

9.a(7). Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Yes

Section 10: Contractor Systems

10.a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

10.a(1). Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(2). The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Agency guidelines.

Yes

Comments: We found one contractor system where SSA did not comply with the Federal requirements for contractor system oversight.

10.a(3). A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

No

Comments: We found three contractor systems not included in the Agency's master systems inventory. The Agency does not have any systems located in a public cloud.

Section 10: Contractor Systems

10.a(4). The inventory identifies interfaces between these systems and Agency-operated systems.

Yes

10.a(5). The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.a(6). The inventory of contractor systems is updated at least annually.

Yes

10.a(7). Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Comments: SSA had 11 contractor systems. We tested 4 systems and found one contractor system where SSA did not comply with the Federal requirements for contractor system oversight.

Section 11: Security Capital Planning

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1). Documented policies and procedures to address information security in the capital planning and investment control process.

Yes

11.a(2). Includes information security requirements as part of the capital planning and investment process.

Yes

11.a(3). Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.a(4). Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

11.a(5). Ensures that information security resources are available for expenditure as planned.

Yes

Section 11: Security Capital Planning

Senior Agency Official For Privacy

Section Report

2011

Annual FISMA Report

Social Security Administration

Question 1: Information Security Systems

	a. Number of Federal systems that contain personal information in an identifiable form			b. Number of systems in column a. for which a Privacy Impact Assessment (PIA) is required under the E-Government Act			c. Number of systems in column b. covered by a current PIA				d. Number of systems in column a. for which a System of Records Notice (SORN) is required under the Privacy Act			e. Number of systems in column d. for which a current SORN has been published in the Federal Register			
Agency/ Component	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	% Complete	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	% Complete
SSA	21	0	21	17	0	17	17	0	17	100%	20	0	20	20	0	20	100%
Agency Totals	***21***	***0***	***21***	***17***	***0***	***17***	***17***	***0***	***17***	***100%***	***20***	***0***	***20***	***20***	***0***	***20***	***100%***

Question 2: Links to PIAs and SORNs

2a. Provide the URL of the centrally located page on the Agency web site that provides working links to Agency PIAs or N/A if not applicable.

http://www.socialsecurity.gov/foia/html/pia.htm

2b. Provide the URL of the centrally located page on the Agency web site that provides working links to the published SORNs or N/A if not applicable.

http://www.socialsecurity.gov/foia/bluebook/toc.htm

Question 3: Senior Agency Official for Privacy (SAOP) Responsibilities

3a. Can your Agency demonstrate with documentation that the SAOP participates in all Agency information privacy compliance activities?

Yes

Comments:

The Office of Privacy and Disclosure (OPD), which the SAOP oversees, is staffed by privacy and disclosure policy specialists who provide guidance on privacy and information disclosure policy to all our components. We participated on the Agency's Personally Identifiable Information (PII) Breach Response Group and the E-Government Steering Committee to ensure privacy compliance. We reviewed, wrote, and amended Privacy Act statements, SORNs, and the PII clauses found in our contracts.

We maintain the Agency's internal Program Operations Manual (POMS) section on Disclosure Policy, and in FY2011 began a comprehensive review of this section to ensure that the guidance is current and includes all Federal and Agency privacy requirements.

For additional information, refer to response to question 9d below.

Question 3: Senior Agency Official for Privacy (SAOP) Responsibilities

3b. Can your Agency demonstrate with documentation that the SAOP participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals, as well as testimony and comments under OMB Circular A-19?

Yes

Comments: The SAOP is involved in the agency's formal review and approval process for establishing agency legislative initiatives involving new privacy policy as well as requests for testimony and comments arising under OMB Circular A-19. The SAOP oversees the agency's regulatory proposals involving privacy policy. In FY 2011, the SAOP reviewed the Patient Protection and Affordable Care Act, and proposed legislative changes to E-Verify, to determine the impact on the agency's privacy requirements.

3c. Can your Agency demonstrate with documentation that the SAOP participates in assessing the impact of the Agency's use of technology on privacy and the protection of personal information?

Yes

Comments: The SAOP approves PIAs assessing the impact of technology on protecting the privacy of personal information. PIAs are part of our Systems Development Lifecycle (SDLC) for all systems. We developed a Privacy Threshold Analysis (PTA) template to assess the privacy risks in new or revised systems or applications and to determine if a PIA or SORN is required. We also partnered with our Office of Systems to acquire software that will examine our web pages for privacy compliance. We assessed the technological impact that several automation projects and applications have on the collection of personal information, including: our Third-Party Social Media applications, the Administrative Law Judge/Public Alleged Misconduct Complaints System, and the Bond Study Systems. The SAOP oversaw and monitored all of these activities.

Question 4: Information Privacy Training and Awareness

Question 4: Information Privacy Training and Awareness

4a. Does your Agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramifications of inappropriate access and disclosure?

Yes

Comments:

We train employees on the Privacy Act and other information privacy laws. Each year we devote significant time and resources hosting privacy education activities on National Data Privacy Day. Our POMS, Chapter GN 033, also contains policy instructions that apply to the disclosure of personal information in our records.

Employees sign a sanctions document annually acknowledging their understanding of the penalties for misusing protected information. We also issue a document to all agency staff entitled "Annual Reminder on Safeguarding Personally Identifiable Information (PII) for SSA Employees," which explains the employee's need to adhere to the Privacy Act and other privacy policies.

We do not routinely grant contractors access to information protected by the Privacy Act or other privacy laws and policies. In the unusual cases where we grant contractors access, we provide application specific training to the contractors who will be accessing the protected information.

4b. Does your Agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) that handle personal information, that are directly involved in the administration of personal information or information technology systems, or that have significant information security responsibilities?

Yes

Comments:

We provide job-specific privacy training to all our employees, including specialized training on the PA, related regulations, policies, and procedures. For instance in FY 2011, we hosted in-depth training on the interface between the PA and the FOIA. Additionally, both management and staff experts attend training conferences hosted by Privacy Interest Groups, OMB, and the CIO Council to ensure that their expertise remains current.
Also, we work closely with the Agency's Office of Learning to develop job-specific training. This fiscal year, we updated the Privacy and Disclosure Online Lesson for our Title II Claims Representative Entry-Level training business initiative.
We use contractors to conduct our security assessments; however, they generally do not have access to PA information while conducting these assessments. If these contractors need access to sensitive information, qualified agency staff oversee the contractors'work.

Question 5: PIA and Web Privacy Policies and Processes

Question 5: PIA and Web Privacy Policies and Processes

5. Does the Agency have a written policy or process for each of the following?

5a. PIA Practices

5a(1). Determining whether a PIA is needed.

Yes

5a(2). Conducting a PIA.

Yes

5a(3). Evaluating changes in technology or business practices that are identified during the PIA process.

Yes

5a(4). Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA.

Yes

5a(5). Making PIAs available to the public as required by law and OMB policy.

Yes

5a(6). Monitoring the Agency's systems and practices to determine when and how PIAs should be updated.

Yes

5a(7). Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained.

Yes

Comments: A standard PTA is now part of the Planning and Analysis phase of our SDLC. The PTA allows us to analyze the need for a PIA or the modification of an existing PIA. The PTA process ensures that the appropriate standards for PIAs are met in accordance with OMB M-03-22 and § 208 of the E-Gov Act.

5b. Web Privacy Practices

5b(1). Determining circumstances where the Agency's web-based activities warrant additional consideration of privacy implications.

Yes

5b(2). Making appropriate updates and ensuring continued compliance with stated web privacy policies.

Yes

Question 5: PIA and Web Privacy Policies and Processes

5b(3). Requiring machine-readability of public-facing Agency web sites (i.e., use of P3P).

Yes

Comments: We routinely conduct PIAs and our written policy for PIAs is incorporated in our SDLC and similar tools that are available throughout the agency. We have posted our machine-readable web privacy policies on our public-facing web pages. In FY2011 we revised our web privacy policy to comply with OMB Memoranda M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies, and M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

Question 6: Mandated Reviews

Component / Bureau	a. Section (m) Contracts	b. Records Practices	c. Routine Uses	d. Exemp-tions	e. Matching Programs	f. Training	g. Violations: Civil Action	h. Violations: Remedial Action	i. System of Records Notices	j. (e)(3) Statement	k. Privacy Impact Assessments and Updates	l. Data Mining Impact Assessment
SSA	X	Y	Y	0	120	Y	Y	Y	102	55	48	X
TOTAL				***0***	***120***				***102***	***55***	48	

Question 7: Written Privacy Complaints

7. Indicate the number of written complaints for each type of privacy issue received by the SAOP or others at the Agency.

7a. Process and Procedural — consent, collection, and appropriate notice.

4

7b. Redress — non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters.

0

7c. Operational — inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction.

0

7d. Referrals — complaints referred to another agency with jurisdiction.

0

Question 8: Policy Compliance Review

Question 8: Policy Compliance Review

8a. Does the Agency have current documentation demonstrating review of the Agency's compliance with information privacy laws, regulations, and policies?

Yes

Comments:

Noteworthy compliance activities: Annual PII/PIA/SORN review; SORN revisions, new SORNS published, reviewed the agency-wide support services contract. We also use the following procedures to comply with information security laws, regulations, and policies:
Our SDLC tests security and privacy controls throughout the system lifecycle.
Our Certification and Accreditation process ensures compliance with established access policies for our information systems predicated on least privilege and need to know.
Our comprehensive Integrity Review Process continuously monitors our employees' access to and use of PA-protected information within our systems.
Our on-site Control and Audit Review process addresses other management controls outside of technical system-based management controls.
We conduct routine security and financial assessments that determine our level of compliance with existing laws, regulations, and policy.
We conduct FISMA- required annual security self-assessments.

8b. Can the Agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?

Yes

Comments:

We have a corrective action mechanism for each of the processes identified in Question 8a that involves tracking and remediating compliance deficiencies.

8c. Does the Agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices?

Yes

Comments:

We use Top Secret history logs to continuously audit our compliance with stated privacy policies and practices. We also use the Audit Tracking System to continuously audit employee compliance.

8d. Does the Agency coordinate with the Agency's Inspector General on privacy program oversight?

Yes

Comments:

Our understanding is that Question 8d applies to agencies subject to section 522 of the Consolidated Appropriations Act of 2005. We are not subject to this provision; however, we work closely with the Inspector General on a variety of privacy issues.

Question 9: Information About Advice and Guidance Provided by the SAOP

Question 9: Information About Advice and Guidance Provided by the SAOP

9. Please select "Yes" or "No" to indicate if the SAOP has provided formal written advice or guidance in each of the listed categories, and briefly describe the advice or guidance if applicable.

9a. Agency policies, orders, directives, or guidance governing the Agency's handling of personally identifiable information.

Yes

Comments: The SAOP, via OPD, provides privacy and disclosure leadership, advocacy, education, and support services that are integral to SSA's mission. We analyze new legislation; maintain and enhance Agency visibility; and interact with the community by participating in special events and conferences. We develop and interpret SSA policy governing the collection, use, maintenance, and disclosure of PII contained in SSA records in accordance with the Privacy Act, the Freedom of Information Act (FOIA), section 1106 of the Social Security Act, section 6103 of the Internal Revenue Code, and other related privacy statutes and regulations. The SAOP collaborates with the OCIO to implement OMB PII guidelines. The SAOP, in conjunction with other agency components, coordinated our FY 2011 review of all PII holdings to ensure such holdings are accurate, relevant, timely, and complete, and to reduce the holdings to the minimum necessary for us to perform our functions.

9b. Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching, and similar issues.

Yes

Comments: OPD and the Office of General Law, under the leadership of the SAOP, review all written data exchange agreements.

9c. The Agency's practices for conducting, preparing, and releasing SORNs and PIAs.

Yes

Comments: The SAOP reviews all practices for PIAs as described in the questions under 5a. The SAOP also reviews all similar practices regarding SORNs, including our recently developed PTA template which helps us to determine whether a new or amended SORN or PIA is required for a system or application.

Question 9: Information About Advice and Guidance Provided by the SAOP

9d. Reviews or feedback outside of the SORN and PIA process (e.g., formal written advice in the context of budgetary or programmatic activities or planning).

Yes

Comments: The SAOP is involved in developing and evaluating rulemaking and agency initiatives with privacy implications, and ongoing application of privacy policy and compliance activities. Working with the SAOP, OPD provides comments on program initiatives or legislative and regulatory proposals that have privacy implications or that impact other statutes and regulations. We provide privacy and disclosure advice during the systems development process. Our participation ensures that we adhere to fair information principles and privacy practices during the planning and development of our IT systems. We help assess the privacy risks of new electronic applications that collect PII from the public to determine the level of user authentication, and to identify any risk that requires mitigation. We also provide privacy guidance to the Agency's Personally Identifiable Information (PII) Breach Response Group and the E-Government Steering Committee.

9e. Privacy training (either stand-alone or included with training on related issues).

Yes

Comments: Under the leadership of the SAOP, we provide general and job-specific privacy training to our employees. Refer to response to questions 4a and 4, above.

Question 10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking technologies")

10a. Does the Agency use web management and customization technologies on any web site or application?

Yes

Comments: We use both Tier 1 (single session) and Tier 2 (multi-session without PII) web measurement and customization technologies, as defined in OMB Memorandum M-l0-22, Guidance for Online Use of Web Measurement and Customization Technologies.

Question 10: Agency Use of Web Management and Customization Technologies (e.g., “cookies,” “tracking technologies”)

10b. Does the Agency annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance?

Yes

Comments: Prior to FY 2010, we did not use web measurement and customization technology as defined by OMB M-00-13, Privacy Policies and Data Collection on Federal Web Sites. Under the new guidelines established by OMB M-l0-22, we conducted an initial survey to determine how best to use the technologies defined under the guidelines. We then assessed the agency's use of these technologies while revising the applicable section of the agency's privacy policy regarding their use. We established a cross-component group to review proposals for new uses of the technology, and to review compliance with OMB's guidelines on an annual basis. We did not identify any issues during our FY 2011 annual review.

10c. Can the Agency demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies?

Yes

Comments: The agency applied for and received approval to use "cookies," as defined by OMB M-00-13. We posted appropriate notice of our use of citizen engagement technologies, disclosed safeguards on our website, and received approval by the head of the agency. Since the release of OMB Memorandum M-l0-22, we performed the activities described in response to question 10b to ensure that we comply with the Memorandum.

10d. Can the Agency provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies?

Yes

Comments: Our web privacy policy concerning the use of web management and customization technologies is available at http://www.ssa.qov/privacy.html.

FY 2011 FISMA

Senior Agency Official for Privacy Report

Agency Efforts to Eliminate Unnecessary Use of SSNs

While the federal government first introduced the Social Security number (SSN) as a means of keeping track of contributions to the Social Security retirement system, both the private and public sectors now widely use the SSN as a personal identifier.

Congress has enacted Federal laws to restrict the use and disclosure of consumers' personal information, including SSNs. Many States have also enacted their own legislation to restrict the use and display of SSNs. However, the agency does not have the legal authority to restrict the use of the SSN. Nevertheless, we have taken several steps to minimize the potential for identity theft involving the SSN. For example, we have:

- removed the SSN from many of the notices we send to the public,
- truncated the SSN to the last 4 digits in many of our internal communications, and
- continued to remind the public via our websites and other forms of communication to keep their SSN card in a secure location.

SOCIAL SECURITY

Office of the General Counsel

MEMORANDUM

Date: April 11, 2011 Refer To: S9H

To: Michael G. Gallagher
Deputy Commissioner
for Budget, Finance and Management

David F. Black
General Counsel
Senior Agency Official for Privacy

From: Daniel F. Callahan
Acting Executive Director
Office of Privacy and Disclosure

Subject: Office of Management and Budget Memorandum M-07-16 Requirement to Review and Reduce Agency Holdings of Personally Identifiable Information (PII) - 2011 Annual Review--Completion

The Office of Management and Budget requires us to review our current holdings of all PII. This requirement ensures such holdings are accurate, relevant, timely, and complete, and reduces them to the minimum necessary for the proper performance of a documented agency function. We completed our FY 2011 review timely, and this memorandum documents our successful completion of this task. Accordingly, no further action is required at this time. We will begin the FY 2012 review later this year.

Should your staff have any questions about this process, please have them contact Dayo Simms of the Office of Privacy and Disclosure at (410) 965-0074.

cc: Chief Information Officer
Associate Commissioner, Office of Publications and Logistics Management

SOCIAL SECURITY

MEMORANDUM

Date: November 14, 2011 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2011 Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act of 2002* (A-14-11-01134)

The attached report summarizes our evaluation of the Social Security Administration's (SSA) Fiscal Year (FY) 2011 information security program and practices, as required by Title III of the *Electronic Government Act of 2002*, Public Law Number 107-347. Title III is also known as the *Federal Information Security Management Act of 2002* (FISMA). FISMA requires that the Office of the Inspector General, or an independent external auditor, conduct an annual evaluation of SSA's information security program and practices.

This report, along with our responses to the FY 2011 Inspector General FISMA reporting questions, is to be submitted through CyberScope pursuant to Office of Management and Budget Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* and Department of Homeland Security, Office of Cybersecurity and Communications Federal Information Security Memorandum 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

SSA continues to demonstrate its commitment as a leader in Federal information protection. We determined that SSA's security programs and practices generally consistent with FISMA requirements for FY 2011; however, there were areas that needed some improvement. We believe the observations outlined in our report will assist SSA management in further strengthening its security program to protect the Agency's valuable information and systems. 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

FISCAL YEAR 2011 EVALUATION OF THE SOCIAL SECURITY ADMINISTRATION'S COMPLIANCE WITH THE *FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002*

November 2011 **A-14-11-01134**

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: November 14, 2011 Refer To:

To: The Commissioner

From: Inspector General

Subject: Fiscal Year 2011 Evaluation of the Social Security Administration's Compliance with the *Federal Information Security Management Act of 2002* (A-14-11-01134)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall security program and practices complied with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) for Fiscal Year (FY) 2011.[1]

BACKGROUND

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB), Department of Homeland Security (DHS), and Congress on the adequacy and effectiveness of their security programs. FISMA requires that each agency develop, document, and implement an agency-wide information security program.[2] OMB and DHS use information reported pursuant to FISMA to evaluate agency-specific and Government-wide security performance and develop the annual security report to Congress.

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 (IS) that fall within FISMA under 44 U.S.C. § 3543.[3] DHS is subject to general OMB oversight in accordance with 44 U.S.C. § 3543(a) and is subject to the limitations and requirements that apply to OMB under 44 U.S.C. § 3543(b)-(c).[4]

---

[1] Pub. L. No. 107-347, Title III, Section 301.

[2] Pub. L. No. 107-347, Title III, Section 301 § 3544(b), 44 U.S.C. § 3544(b).

[3] OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security,* July 6, 2010.

[4] Id.

On September 14, 2011, OMB issued its FY 2011 FISMA reporting guidance,[5] which incorporated DHS' August 24, 2011 Federal Information Security Memorandum (FISM) 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. FISM 11-02 provided FY 2011 FISMA reporting instructions to Federal Chief Information Officers, Inspectors General (IG), and Senior Agency Officials for Privacy. DHS continues to require that Chief Information Officers, IGs, and Senior Agency Officials for Privacy use a Web platform, CyberScope, to submit FISMA reports and data.

We evaluated SSA's information security program to determine whether the Agency established and maintained key information security programs and practices as identified by DHS.[6] DHS' 11 key FISMA programs and metrics and our responses are in Appendix B. Also, see Appendix C for additional background.

SCOPE AND METHODOLOGY

FISMA directs each agency's IG or an independent external auditor, as determined by the agency's IG, to perform an annual, independent evaluation of the effectiveness of the agency's information security program and practices.[7] SSA's Office of the Inspector General (OIG) contracted with Grant Thornton LLP (GT) to audit SSA's FY 2011 financial statements.[8] Because of the extensive internal control system review that is completed as part of that work, our FISMA requirements were incorporated into GT's financial statement information technology-related work. This evaluation included the *Federal Information System Controls Audit Manual* level reviews of SSA's financial-related information systems. GT also performed an "agreed-upon procedures" engagement using FISMA, OMB, DHS, National Institute of Standards and Technology (NIST) guidance, *Federal Information System Controls Audit Manual*, and other relevant security laws and regulations as a framework to provide information and documentation for the required OIG review of SSA's information security program, practices, and information systems.

This report informs Congress and the public about SSA's security performance and fulfills the OMB requirement under FISMA to submit an annual report to Congress. It provides an assessment of SSA's information security strengths and weaknesses and a plan of action to improve performance. See Appendix D for more details on our scope and methodology.

---

[5] OMB Memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 14, 2011.

[6] DHS, *FY 2011 Inspector General Federal Information Security Management Act Reporting*, Version 1.0, June 1, 2011.

[7] Pub. L. No. 107-347, Title III, Section 301, 44 U.S.C. § 3545(b)(1).

[8] OIG Contract Number GS-23F-8196H, December 3, 2009. The FY 2011 option was exercised in December 2010.

SUMMARY OF RESULTS

OIG and GT's work determined that SSA's security programs and practices were generally consistent with FISMA requirements for FY 2011;[9] however, there were some areas that needed improvement. SSA continues to work toward maintaining a secure environment for its information and systems. For example, SSA continues to have generally consistent processes in a number of areas, including risk management, vulnerability remediation, security training, remote access, continuous monitoring (CM), security capital planning, and account and identity management. Our responses to the FY 2011 DHS IG metrics are in Appendix B. We used these metrics to evaluate SSA's compliance with FISMA for FY 2011.

Although the Agency continues to protect its information and systems, the FY 2011 financial statement audit again identified a significant deficiency for financial statement reporting. It should be noted that a financial statement significant deficiency in internal control[10] does not necessarily rise to the level of a significant deficiency as defined in FISMA.[11] The FY 2011 financial statement audit significant deficiency does not rise to the level of a significant deficiency under FISMA because of other compensating controls the Agency has in place, such as intrusion detection systems, guards, closed circuit televisions, automated systems checks, configuration management, and firewalls.

---

[9] See Appendix B.

[10] The definition of **a significant deficiency for financial statement internal control** is provided by the Statement on Auditing Standards Number 115, *Communicating Internal Control-Related Matters Identified in an Audit.* This Statement on Auditing Standards states a significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis.

[11] DHS provided the definition of **a significant deficiency under FISMA** in FISM 11-02. The Frequently Asked Questions section, p. 8. defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

Although we concluded that SSA's security programs were generally consistent with FY 2011 FISMA requirements, our review found areas where SSA can improve the security over its systems and protection of sensitive information. SSA should ensure

- continued improvements in change and access control processes;
- continued improvements in its risk management process;
- proper incident handling and reporting;
- protection of personally identifiable information (PII);[12]
- contractors receive security awareness and specialized training;
- continued implementation of its CM strategy; and
- contractor system oversight.

CONTINUED IMPROVEMENTS IN CHANGE AND ACCESS CONTROL PROCESSES

OMB Circular A-123 Significant Deficiency

Controlling and limiting systems access to the Agency's information systems and resources is the first line of defense in ensuring the confidentiality, integrity, and availability of the Agency's information resources.[13] Lack of adequate access controls compromises the completeness, accuracy, and validity of the information in the system.

In FY 2009, our audit of SSA's financial statements identified a significant deficiency[14] in the Agency's control of access to its sensitive information.[15] In FYs 2010 and 2011, GT's audit of SSA's financial statements continued to identify a significant deficiency in the Agency's change control management and access to sensitive information.[16] Specifically, GT's FY 2011 testing disclosed that SSA developed policies and procedures for periodically reassessing the content of security access profiles but has not implemented them consistently Agencywide. In addition, SSA provided some employees and contractors more security permissions than required to complete their job responsibilities. Furthermore, GT found that some of the Agency's software

---

[12] OMB, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* p. 1, July 2006, 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 that 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.

[13] SSA, *Information Systems Security Handbook*, Section 2.1.

[14] See Footnote 10.

[15] SSA OIG, *Independent Auditor's Report* on SSA's FY 2009 Financial Statements, November 9, 2009.

[16] GT, *Independent Auditor's Report* on SSA's FY 2010 Financial Statements, November 8, 2010 and GT, *Independent Auditor's Report* on SSA's FY 2011 Financial Statements, November 7, 2011.

configurations increased the risk of unauthorized access to SSA's key financial data and programs.[17]

GT recommended that SSA management implement (1) policies and procedures that require a periodic review of the content of all security profiles,[18] (2) controls to test and monitor configurations on the mainframe and network operating system environments, and (3) procedures that require ongoing monitoring of implemented configurations to identify and address security risks.[19]

In FY 2011, SSA issued two policies[20] and assembled a workgroup to address the access control weaknesses identified in prior years. The workgroup is testing a commercial tool to manage SSA employee and contractor access. The Agency stated that it is finalizing the profile reviewing procedures. In addition, the new tool, when implemented, will automate the process SSA uses to review its security profiles. SSA plans to implement the tool in the second quarter of FY 2012 to resolve some of its access control weaknesses.

CONTINUED IMPROVEMENTS IN ITS RISK MANAGEMENT PROCESS

We found SSA's risk management[21] program was generally consistent with FY 2011 FISMA requirements.[22] NIST guidance indicates that the Risk Management Framework steps include, among other things, categorizing an agency's IS and the information processed, stored, and transmitted by that IS; selecting and implementing proper IS security controls; and assessing the effectiveness of these controls.[23] Once IS controls

---

[17] GT, *Independent Auditor's Report* on SSA's FY 2011 Financial Statements, November 7, 2011.

[18] A profile is one of SSA's primary access control mechanisms. Each profile contains a unique mix of facilities and transactions that determines what access to systems resources that specific position needs.

[19] See Footnote 17.

[20] SSA, *Security Profile Administration Processes Final Mainframe Administration Standards*, May 10, 2011, and SSA, *Security Profile Administration Processes Profile Naming Conventions*, October 28, 2010.

[21] NIST Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Appendix B, February 2010 p. B-8, defines risk management as "The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system."

[22] See Appendix B, Section 1.

[23] NIST SP 800-37, Revision 1, supra at pp. 7 and 8.

are selected and tested, the IS undergoes a security authorization process to obtain an approval to operate.[24]

We determined SSA had conducted security authorizations[25] for its 21 major systems and applications[26] in the past 3 years. Further, we reviewed four of the six major systems or applications that underwent a security authorization in FY 2011 and found the process was generally consistent with OMB and NIST guidance. DHS guidance provides that the security authorization process formally authorizes a system to operate and provides a systematic approach for assessing security controls to determine their overall effectiveness.[27] However, SSA stated that because of budget cuts, it did not update the System Security Plans (SSP)[28] for two major systems, FALCON Data Entry System and Security Unified Measurement System, or perform annual security control testing for these two systems, as required by FISMA.[29]

The FALCON Data Entry System is used in SSA's processing centers to correct or update mass amounts of SSA benefit payment data by manual data entries. Security Unified Measurement System provides SSA managers and analysts information required to meet strategic business needs, support process reviews and support compliance with government standards for cost accountability. Because the SSPs were not updated and the annual security controls were not tested, the Agency cannot ensure (1) the two SSPs continue to reflect the correct security information about the system and (2) key security controls continue to operate effectively and efficiently to protect the confidentiality, integrity, and availability of the data contained in these systems.

FY 2011 FISMA guidance states, ". . . Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of CM programs."[30] FISMA guidance

---

[24] Id.

[25] 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."

[26] See Appendix E for a list and definitions of the 21 major systems and applications.

[27] DHS FISM 11-02, supra, Frequently Asked Questions, Question 25, at p. 10.

[28] NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, p. 39, defines System Security Plan as a "Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements."

[29] Pub. L. No. 107-347, Title III, Section 301 § 3544(b)(5), 44 U.S.C. § 3544(b)(5).

[30] DHS FISM 11-02, supra, Frequently Asked Questions, Question 28, p. 10.

also states, “Agency officials should monitor the security state of their information systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their organizations.”[31] Finally, FISMA guidance indicates that a CM program will help make the security authorization process more dynamic and responsive to today’s Federal missions and rapidly changing conditions.[32]

We found SSA was transitioning to this new dynamic process. As of September 2011, SSA had issued its CM strategy to establish, implement, and maintain a more robust and near real-time program (see additional information in the section related to CM). In the future, we will assess how SSA integrates its CM program with its security authorization program.

PROPER INCIDENT HANDLING AND REPORTING

SSA’s Incident Handling and Reporting program was generally consistent with FY 2011 FISMA requirements.[33] SSA implemented an automated PII Loss Reporting tool[34] to ensure compliance with Federal requirements and address our prior year finding related to SSA’s PII incident reporting timeframe.[35] Additionally, we found SSA reported 100 percent of the PII incidents included in our FY 2011 sample to the United States Computer Emergency Readiness Team (US-CERT) within 1 hour.[36] However, our review identified the following weaknesses.

- We did not receive any reports of PII incidents for FY 2011.
- SSA policy did not establish a law enforcement reporting timeframe.

FISMA requires that agencies notify and consult law enforcement agencies and their OIGs regarding security incidents, as appropriate.[37] FISMA did not define what security

---

[31] DHS FISM 11-02, supra, Frequently Asked Questions, Question 28, p. 11.

[32] DHS FISM 11-02, supra, Frequently Asked Questions, Question 32, p. 12.

[33] See Appendix B, Section 3.

[34] In FY 2010, the Office of the Chief Information Officer implemented an automated PII Loss Reporting tool to enable SSA to report a higher percentage of PII incidents to US-CERT within 1 hour.

[35] OMB guidance requires that agencies report to US-CERT within 1 hour of discovery/detection any unauthorized access to PII or any incident involving PII when (1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or (2) there is a suspected or confirmed breach of PII regardless of the manner in which it might have occurred. OMB, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, p. 10.

[36] In FY 2010, according to a sample we tested, SSA reported 80 percent of PII incidents to US-CERT within 1 hour.

[37] Pub. L. No. 107-347, Title III, Section 301 § 3544(b)(7)(C)(i), 44 U.S.C. § 3544(b)(7)(C)(i).

incidents are appropriate to be reported to law enforcement or the OIG. Instead, Federal guidance[38] advises agencies to discuss with various law enforcement representatives conditions under which incidents should be reported to law enforcement and OIG, how the incidents should be reported, what evidence should be collected, and how the evidence should be collected.

In FYs 2009 and 2010, we reported SSA did not report any PII-related incidents to the OIG. We also found SSA's policy and procedures did not provide guidance on what type of security incidents and in what timeframe these incidents must be reported to law enforcement and the OIG. We identified the same conditions in FY 2011. Although specific guidance had not been developed, we believe, at a minimum, all security incidents SSA deemed appropriate to be reported to law enforcement should have been reported to us.

To resolve this issue, the Agency is working with the OIG's Office of Technology and Resource Management to establish guidance for reporting specific security-related incidents, including PII. Additionally, the Agency developed its PII Loss Reporting Tool to automatically notify the OIG's Office of Technology and Resource Management of PII incidents. However, the OIG did not receive any reports of PII incidents in FY 2011 because of an incorrect email address incorporated into SSA's PII Loss Reporting Tool.

Because SSA did not refer any incidents to OIG for investigation, we could not conduct any additional investigation, if needed. As a result, we could not conclude that SSA timely resolved these incidents to minimize future damage.[39] We continue to recommend SSA:

1. Work with the OIG to establish policy and procedures on what types of PII incidents should be reported to law enforcement and the OIG and in what timeframes.
2. Revise its policy, guidance, procedures, and timeframes for reporting of PII incidents to law enforcement, including the OIG.

PROTECTION OF PII

The Privacy Act of 1974[40] requires that Federal agencies safeguard PII. In addition, FISMA requires that agencies protect their information from unauthorized disclosure[41]

---

[38] NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide,* Section 2.3.4.2, March 2008, p. 2-6.

[39] See Appendix B, 3.a(5).

[40] Pub. L. No. 93-579, as amended, § 552a(e)(10), 5 U.S.C. § 552a(e)(10).

[41] FISMA requires that agencies protect information collected or maintained by, or on behalf of, agencies commensurate with the risk and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction. Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A)(i), 44 U.S.C. § 3544(a)(1)(A)(i).

and OMB has issued several memorandums on how agencies should safeguard PII.[42] Although SSA has established policies and procedures for PII protection, we noted an opportunity for improvement.

We performed a follow-up audit that identified a breach of PII from the Agency's publication of its Death Master File (DMF).[43] We found that SSA continued publishing the DMF with knowledge that the DMF contents included PII of living individuals. SSA stated it could not limit the information included in the DMF version sold to the public to the absolute minimum required because deceased individuals do not have privacy interests. The Agency also stated that the number of DMF errors was small relative to the number of death transactions, and that SSA had no evidence of Social Security number misuse related to these DMF errors. Further, SSA implemented procedures to report erroneous death entry-related PII breaches to US-CERT each week. However, we remain concerned about the potential for harm to the living individuals whose PII is, and will be, published in the DMF.

SSA stated that it holds sensitive information about hundreds of millions of people in its records. SSA further stated while it takes even a small error rate very seriously, focusing on the DMF belies the Agency's success in protecting the privacy of sensitive information contained in its records.

CONTRACTORS RECEIVE SECURITY AWARENESS AND SPECIALIZED TRAINING

SSA's security training program was generally consistent with FY 2011 FISMA requirements.[44] SSA made some improvements in its security training program. SSA developed additional role-based training guidance for personnel with significant security responsibilities in FY 2011. Additionally, the Agency required that its employees complete their FY 2011 annual security awareness training through an automated interactive program. Moreover, in FY 2012, the Office of Information Security (OIS) is strengthening its training program by creating and delivering managerial and executive information security training in FY 2012.

However, we found the Agency did not require that contractors complete annual security awareness training through this interactive program. The Agency plans to

---

[42] OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006; M-06-16, *Protection of Sensitive Agency Information,* June 23, 2006; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; and M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

[43] SSA OIG, *Follow-up: Personally Identifiable Information Made Available to the Public Via the Death Master File* (A-06-10-20173), March 2011. SSA maintains a record of reported deaths known as the DMF, which is provided to public and private customers.

[44] See Appendix B, Section 4.

require that contractors use this automated program next FY. Although the Agency's security training program is generally consistent with FY 2011 FISMA requirements, we identified some weaknesses related to security training for SSA's contractors.

- SSA did not ensure all contractor personnel received and completed annual security awareness training.[45]
- SSA did not maintain a comprehensive list of all contractors with significant security responsibilities; as a result, SSA could not ensure all such contractors received appropriate specialized training.[46]

SSA policy requires that contractor personnel annually sign a *Personnel Security Certification* form to certify completion and comprehension of the Agency's security awareness training requirements.[47] We requested the *Personnel Security Certification* forms for a sample of 30 contractors. SSA provided 11 forms. For the other 19, the Agency had 11 contractors sign and date the form after our request but did not provide the other 8 forms. We also found that SSA did not define a timeframe for each contractor to complete the certification form.

As a result, contractors may have access to systems and data without proper security training and certification. In addition, we do not believe the contractor's signature on the certification form is an effective control for ensuring the contractor took the appropriate security awareness training, because the contractor could sign the form without taking the training.

---

[45] FISMA requires each agency head to ensure that that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter [44 USCS §§ 3541 et seq.] and related policies, procedures, standards, and guidelines. It also requires agencies to have an agency-wide information security program that includes security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of--

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks. Pub. L. No. 107-347, Title III, Section 301(b) §§ 3544(a)(4) and (b)(4), 44 U.S.C. §§ 3544(a)(4) and (b)(4). In addition, NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003, Footnote 13, p. 20, states "[a]t a minimum, the entire workforce should be exposed to awareness material annually."

[46] FISMA requires that the agency Chief Information Officer ensure compliance with FISMA requirements, including training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities. Pub. L. No. 107-347, Title III, Section 301(b) § 3544(a)(3)(D), 44 U.S.C. § 3544(a)(3)(D).

[47] SSA, *Information Systems Security Handbook*, Appendix B, Roles and Responsibilities.

Further, we could not determine whether SSA's *contractors* with significant information security responsibilities[48] received specialized training or whether such training contained appropriate content based on organizational roles. We requested, but were unable to obtain, a comprehensive list of contractors with significant information security responsibilities. SSA staff stated that the Agency does not have sufficient guidance on categorizing contractors with significant information security responsibilities. Moreover, SSA staff stated that each component subjectively categorized contractors with significant information security responsibilities. As a result, SSA could not provide a comprehensive list that included all contractors with significant information security responsibilities and SSA does not know whether all such contractors received appropriate specialized training.

We recommend SSA establish a timeframe for contractor personnel to complete security awareness training. Furthermore, the Agency should ensure all contractor personnel complete security awareness training before gaining access to Agency systems. In addition, we recommend the Agency provide additional guidance to assist SSA components to identify contractors with significant information security responsibilities and ensure these contractors received specialized training.

[48] SSA defined its employees and contractors with significant security responsibilities as Level 3 personnel. Level 3 personnel are "Employees with high levels of access to sensitive data who could affect agency-wide operations and/or who perform security, investigative, or auditing activities on a frequent basis. Personnel in these roles have significant access to sensitive information, such as social security records, medical records, business confidential documents, and other personally identifiable information, which needs to be protected against unauthorized access; fraudulent activities; and inappropriate disclosure and modification." SSA, *Information Systems Security Handbook*, Appendix H, *Security Training*.

CONTINUED IMPLEMENTATION OF ITS CM STRATEGY

SSA's CM program was generally consistent with FY 2011 FISMA requirements.[49] NIST established new guidelines for CM in August 2009.[50] The NIST control for CM provides that the organization establishes a CM strategy and implements a CM program that includes

- a configuration management process for the IS and its constituent components;
- a determination of the security impact of changes to the IS and the environment of operation;
- ongoing security control assessments in accordance with the organizational CM strategy; and
- reporting the security state of the IS to appropriate organizational officials.[51]

SSA has documented CM policies and procedures and developed and issued its *Strategy for Information Security Program Continuous Monitoring,* on September 16, 2011 to ensure compliance with all new requirements related to CM. The strategy is driven by the need to dynamically monitor the Agency's security posture and provide real-time awareness of threats, vulnerabilities, and risks. This strategy identified gaps between the Agency's existing CM program and existing and anticipated requirements and provided a road map to achieve SSA's goals.

In addition, SSA has implemented CM for most of its core information processing environment.[52] While SSA generally had a consistent CM program and process, we determined there were opportunities for improvement in the Agency's CM program and process in the following areas.

---

[49] See Appendix B, Section 8.

[50] NIST, SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, pp. F-36 and F-37, August 2009. This guidance also provides that: "A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the impact level of the information system."

[51] NIST SP 800-53, Revision 3, supra at pp. F-36 and F-37.

[52] SSA *Enterprise Wide Mainframe & Distributed Network Telecommunications Services System (EWANS) System Security Plan (SSP),* Section 1.10, defines core information processing environment as a combination of mainframe processors, UNIX computers, Microsoft Windows servers and desktops for its core information processing, p. 4, September 28, 2011.

- SSA had not implemented a CM process for some of its servers in FY 2011 because it finalized the configuration guide for these servers in September 2011.
- Some of SSA's CM data were not readily accessible to the Chief Information Security Officer (CISO).[53] For example, the reportable data for SSA's configuration and vulnerability management tools for mainframe and some network assets is not readily accessible to the CISO.

Moreover, in SSA's FY 2009 Financial Statement Audit, GT identified that SSA did not have a formal process to detect and remove unauthorized software from all of its workstations. Our prior evaluation identified a similar finding.[54] This issue continues to exist in FY 2011. The above weaknesses may negatively impact SSA's ability to correctly measure and timely remediate security vulnerabilities. For example, GT's internal penetration testing[55] performed during its audit of SSA's FY 2011 financial statements identified some security weaknesses. We communicated the details of these weaknesses to the Agency. SSA is implementing CM tools for some of these weaknesses. However, these security weaknesses may have been discovered had the Agency implemented additional CM process for some of its applications and servers sooner. Further, the limited accessibility of CM data provided to SSA's CISO may impact his effectiveness to oversee the Agency's security program.

In addition, although NIST guidance promotes the concept of near real-time risk management,[56] SSA has limited real-time automated monitoring and reporting capacity. As indicated in SSA's CM strategy, the absence of automated tools makes security metrics difficult to generate and labor intensive, and there are increased opportunities for human error. Adopting automated tools that consolidate CM information will reduce the burden of collecting data, increase the quality of data, and promote near real-time CM.

---

[53] OMB guidance states that "[a]gencies need to be able to continuously monitor security-related information from across the enterprise in a manageable and actionable way. Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and other Agency management all need to have different levels of this information presented to them in ways that enable timely decision making." OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* p. 1, April 21, 2010.

[54] OIG reported SSA employees and contractors did not comply with the Agency's software approval policy. SSA OIG, *The Social Security Administration's Approval and Monitoring of the Use of Software,* (A-14-10-21082), October 2010, p.4.

[55] Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. Internal penetration testing during SSA's financial statement audit was performed by a tester as an "insider" without specific information about SSA information systems environment and with access to SSA facilities.

[56] NIST SP 800-37, Revision 1, supra at p. 2 and NIST SP 800-53, Revision 3, supra at p. F-36.

NIST guidance provides that ". . . [t]he implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions."[57]

We recommend SSA ensure implementation of its *Strategy for Information Security Program Continuous Monitoring* to fully meet the current and anticipated Federal requirements and address all gaps identified in the CM strategy and this report. In addition, SSA should ensure the CISO has access to all Agency CM data.

CONTRACTOR SYSTEM OVERSIGHT

We determined SSA's contractor system[58] oversight program was generally consistent with FISMA requirements for FY 2011.[59] However, we identified some areas that need improvement. We found the following weaknesses.

- SSA's Master System Inventory did not identify all contractor systems.
- SSA did not ensure that all contractor systems met FISMA requirements before putting them into operation.
- SSA's contracts still did not include all FISMA requirements. [60]

SSA's FY 2011 Master System Inventory identified eight contractor systems. However, we found this inventory did not include all contractor systems.[61] These systems are a card production system, operated by a SSA contractor; E2 Solutions, operated by the General Services Administration;[62] and Cyber Security Assessment and Management (CSAM),[63] operated by the Department of Justice.[64]

SSA stated E2 Solutions and CSAM should be excluded from the Agency's inventory because (1) SSA is not responsible for the security authorization of the two systems,

---

[57] NIST SP 800-37, Revision 1, supra at p. 26.

[58] Contractor systems are provided or managed by another agency, contractor, or other source.

[59] See Appendix B, Section 10.

[60] OMB M-11-33, supra, Frequently Asked Questions section, Question 38, pp. 14 and 15.

[61] SSA did not include CSAM and E2 Solutions in its system inventory.

[62] E2 Solutions is the travel system adopted by SSA.

[63] CSAM is SSA's FISMA tracking tool. CSAM enables the Agency and SSA's C&A Managers to gather system information and to create reports to support the FISMA assessment. SSA also uses CSAM for managing the identified information security weaknesses.

[64] In FY 2011, OIG found the Agency excluded CSAM and E2 Solutions from the inventory.

and (2) SSA has no "system-to-system" connection with CSAM. However, FISMA specifically requires that each 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 by a contractor of an agency or other organization on behalf of an agency.[65] In addition, NIST guidance defers to OMB to provide guidance for the agency system inventory development and associated reporting requirements.[66] DHS began exercising FISMA responsibilities on behalf of OMB. DHS guidance requires the OIG to evaluate whether the Agency has established a program that includes a complete inventory of systems operated by contractors or other entities on the Agency's behalf.[67]

As a result, we believe SSA should include these systems in its Master Systems Inventory because SSA needs to ensure it obtains sufficient assurance that security controls of such systems are effectively implemented and comply with Federal and Agency guidelines.[68]

Moreover, for FY 2011, we found that SSA performed steps to confirm that the Department of Justice and the General Services Administration completed the security authorization for E2 and CSAM. However, the Agency did not perform steps to confirm that the contractor card production system had a security authorization.

We discussed this issue with the OIS. OIS staff stated although the contractor system is part of SSA's Security Management Access Control System[69] (SMACS), the Agency decided not to include the contractor system as a subsystem of SMACS because there was no direct "system-to-system" connection between SSA and the contractor but simply information sharing. As a result, SSA did not ensure completion of a security authorization for this system.

We do not agree with OIS. The contractor system processes PII used to create SSA's Homeland Security Presidential Directive 12[70] (HSPD-12) employee and contractor

---

[65] Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A), 44 U.S.C. § 3544(a)(1)(A). FISMA provides for such protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of such information. Id.

[66] NIST SP 800-53, Revision 3, supra at page G-3, PM-5.

[67] DHS, *FY 2011 Inspector General FISMA Reporting*, Version 1.0, § 10.a(3), June 1, 2011.

[68] DHS, supra, § 10.a(2).

[69] SMACS is a major Agency application that securely gathers and stores privacy-related data for employment and, in certain cases, clearances.

[70] HSPD-12 requires the development and implementation of a mandatory, Government-wide standard for secure and reliable forms of identification for Federal employees and contractors. OMB M-05-24 *Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Contractors,* August 5, 2005, p.1.

credentials. As part of the credential creation process, SSA electronically transmits data files[71] containing PII to the contractor for the production of the credentials. At the end of the process, SSA receives the HSPD-12 credentials containing PII for its employees and contractors.

In addition, the SMACS SSP describes the contractor's services provided to SSA to implement the Agency's HSPD-12 program. Federal HSPD-12 guidance requires that all systems involved in the HSPD-12 process comply with security authorization requirements.[72] Since the contractor's system is used to implement HSPD-12, the system must comply with the security authorization requirements.

Further, in one of our current reviews,[73] we found SSA did not conduct a security authorization on this contractor system or obtain sufficient assurance that appropriate controls were implemented and working effectively to protect the PII entrusted to the contractor. In addition, SSA did not include all FISMA security requirements in the contract. Although we found the contractor had implemented security controls, SSA could not require that the contractor continue maintaining these controls without the proper contract requirements.

We reiterate our prior recommendations for SSA to include all contractor systems in its system inventory and ensure all appropriate contracts include Federal security requirements.

CONCLUSIONS AND RECOMMENDATIONS

Based on the results of OIG and GT's work, we believe SSA's information security programs and practices were generally consistent with FISMA requirements; however, some improvements are needed. SSA continues to work with us to identify ways of complying with FISMA. The Agency continues developing, implementing, and operating security controls to protect its sensitive data, assets, and operations.

In our prior FISMA reports, we identified issues related to SSA's (1) computer security program, (2) access controls, (3) strategic planning, (4) protection of PII, (5) vulnerability remediation process, (6) contractor security awareness training, (7) incident reporting, (8) security authorization process, (9) contingency planning, and (10) contractor systems oversight. We affirm our prior recommendations in these areas and encourage the Agency to continue to implement them.

SSA should continue strengthening its overall security program and practices and

---

[71] The files contain SSA employee or contractor's first name, middle initial, last name, card expiration date, agency affiliation, and photograph.

[72] Federal Information Processing Standards Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, March 2006, p. 64.

[73] SSA OIG, *Contractor Security of the Social Security Administration's Homeland Security Presidential Directive-12 Credentials* (A-14-11-11106). This report has not been issued to date..

ensure future compliance with FISMA and other information security related laws and regulations. Therefore, we recommend SSA:

1. Establish a timeframe for contractor personnel to complete security awareness training and ensure all contractor personnel complete security awareness training before being granted access to Agency systems;
2. Provide additional guidance to assist SSA components to identify contractors with significant information security responsibilities and ensure these contractors received specialized training;
3. Ensure implementation of its *Strategy for Information Security Program Continuous Monitoring* to fully meet the current and anticipated Federal requirements and address all gaps identified in the strategy and this report; and
4. Ensure the CISO has access to all Agency CM data.

Patrick P. O'Carroll, Jr.

Appendices

Acronyms

CISO	Chief Information Security Officer
CM	Continuous Monitoring
CSAM	Cyber Security Assessment and Management
DHS	Department of Homeland Security
DMF	Death Master File
FISM	Federal Information Security Memorandum
FISMA	*Federal Information Security Management Act of 2002*
FY	Fiscal Year
GT	Grant Thornton LLP
HSPD-12	Homeland Security Presidential Directive 12
IG	Inspector General
IS	Information Systems
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
POA&M	Plan of Action and Milestones
SMACS	Security Management Access Control System
SP	Special Publication
SSA	Social Security Administration
SSP	System Security Plan
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Appendix B

Office of the Inspector General Response to *Federal Information Security Management Act of 2002* Metrics

Section 1: RISK MANAGEMENT

1.a. The Agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

1.a(1) Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.

Yes

1.a(2) Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1.

Yes

1.a(3) Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1.

Yes

1.a(4) Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1.

Yes

1.a(5) Categorizes information systems in accordance with government policies.

Yes

1.a(6) Selects an appropriately tailored set of baseline security controls.

Yes

1.a(7) Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

Comments: Due to budget cuts, the Social Security Administration (SSA) stated that it did not update the System Security Plans for two of its general support systems and did not perform annual security tests on them.

1.a(8) Assesses the security controls using appropriate assessment procedures 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.

Yes

1.a(9) Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

Yes

1.a(10) Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Yes

1.a(11) Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

1.a(12) Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

1.a(13) Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

Yes

1.a(14) Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

Yes

Section 2: CONFIGURATION MANAGEMENT

2.a. The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

2.a(1) Documented policies and procedures for configuration management.

Yes

2.a(2) Standard baseline configurations defined.

Yes

Comments: The Agency has established baseline configurations for most, but not all environments. SSA does not have configuration baselines for two systems.

2.a(3) Assessing for compliance with baseline configurations.

Yes

Comments: We identified some weaknesses with SSA's monitoring of configuration settings.

2.a(4) Process for timely, as specified in Agency policy or standards, remediation of scan result deviations.

Yes

2.a(5) For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

Yes

2.a(6) Documented proposed or actual changes to hardware and software configurations.

Yes

2.a(7) Process for timely and secure installation of software patches.

Yes

Section 3: INCIDENT RESPONSE AND REPORTING

3.a. The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

3.a(1) Documented policies and procedures for detecting, responding to and reporting incidents.

Yes

Comments: SSA can improve its incident response and reporting program by establishing additional guidance on reporting incidents to the Office of the Inspector General (OIG) and law enforcement.

3.a(2) Comprehensive analysis, validation and documentation of incidents.

Yes

3.a(3) When applicable, reports to US-CERT within established timeframes.

Yes

3.a(4) When applicable, reports to law enforcement within established timeframes.

No

Comments: SSA does not have an established timeframe for reporting incidents to law enforcement or the OIG. Additionally, SSA did not report any PII incidents to OIG due to an incorrect email address in its system.

3.a(5) Responds to and resolves incidents in a timely manner, as specified in Agency policy or standards, to minimize further damage.

Yes

Comments: SSA reports security incidents to the United States Computer Emergency Readiness Team timely. However, SSA has not established a timeframe to report security related incidents to law enforcement and the OIG. In addition, OIG did not receive any referrals for further investigation.

3.a(6) Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

Comments: SSA does not use virtual/cloud environments.

3.a(7) Is capable of correlating incidents.

Yes

Section 4: SECURITY TRAINING

4.a. The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

4.a(1) Documented policies and procedures for security awareness training.

Yes

4.a(2) Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

4.a(3) Security training content based on the organization and roles, as specified in Agency policy or standards.

Yes

4.a(4) Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Agency users) with access privileges that require security awareness training.

No

Comments: SSA currently does not track security awareness training for contractors. SSA stated it would have an automated system to track security awareness training next fiscal year.

4.a(5) Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Agency users) with significant information security responsibilities that require specialized training.

No

Comments: SSA was not able to provide a comprehensive list of contractors with significant information security responsibilities. Therefore, we were unable to test this area.

Section 5: POA&M

5.a. The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

5.a(1) Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

Yes

5.a(2) Tracks, prioritizes and remediates weaknesses.

Yes

5.a(3) Ensures remediation plans are effective for correcting weaknesses.

Yes

5.a(4) Establishes and adheres to milestone remediation dates.

Yes

5.a(5) Ensures resources are provided for correcting weaknesses.

Yes

5.a(6) Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.

Yes

Section 6: REMOTE ACCESS MANAGEMENT

6.a. The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

6.a(1) Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

6.a(2) Protects against unauthorized connections or subversion of authorized connections.

Yes

6.a(3) Users are uniquely identified and authenticated for all access.

Yes

6.a(4) If applicable, multi-factor authentication is required for remote access.
Yes

6.a(5) Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

6.a(6) Defines and implements encryption requirements for information transmitted across public networks.

Yes

6.a(7) Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required.

Yes

Section 7: IDENTITY AND ACCESS MANAGEMENT

7.a. The Agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

7.a(1) Documented policies and procedures for account and identity management.

Yes

7.a(2) Identifies all users, including federal employees, contractors, and others who access Agency systems.

Yes

7.a(3) Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

7.a(4) If multi-factor authentication is in use, it is linked to the Agency's PIV program where appropriate.

Yes

7.a(5) Ensures that the users are granted access based on needs and separation of duties principles.

Yes

Comments: We identified some weaknesses with SSA's process to ensure that users are granted access based on need and the separation of duties principles.

7.a(6) Identifies devices that are attached to the network and distinguishes these devices from users.

Yes

Comments: We identified some weaknesses with SSA's process to identify devices attached to its network.

7.a(7) Ensures that accounts are terminated or deactivated once access is no longer required.

Yes

Comments: We identified some weaknesses with SSA's process to ensure that accounts are terminated or deactivated once access is no longer required.

7.a(8) Identifies and controls use of shared accounts.

Yes

Comments: SSA stated that it does not allow users to share accounts.

Section 8: CONTINUOUS MONITORING MANAGEMENT

8.a. The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

8.a(1) Documented policies and procedures for continuous monitoring.

Yes

8.a(2) Documented strategy and plans for continuous monitoring.

Yes

8.a(3) Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.

Yes

Comments: SSA has not implemented configuration monitoring tools for some of its servers.

8.a(4) Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans.

Yes

Comments: There are Continuous Monitoring data not readily accessible to SSA's Chief Information Security Officer.

Section 9: CONTINGENCY PLANNING

9.a. The Agency established and is maintaining an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

9.a(1) Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.

Yes

9.a(2) The Agency has performed an overall Business Impact Analysis (BIA).

Yes

Comments: SSA's last Business Impact Analysis was conducted in 2004.

9.a(3) Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

Comments: The contingency plan for one system has remained in draft form since Fiscal Year 2008.

9.a(4) Testing of system specific contingency plans.

Yes

Comments: SSA's disaster recovery exercise included 19 of the Agency's 21 major systems and applications.

9.a(5) The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.a(6) Development of test, training, and exercise (TT&E) programs.

Yes

9.a(7) Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Yes

Section 10: CONTRACTOR SYSTEMS

10.a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

10.a(1) Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

Yes

10.a(2) The Agency obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and agency guidelines.

Yes

Comments: We found one contractor system where SSA did not comply with the Federal requirements for contractor system oversight.

10.a(3) A complete inventory of systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud.

No

Comments: We found three contractor systems not included in the Agency's master systems inventory. The Agency does not have any systems located in a public cloud.

10.a(4) The inventory identifies interfaces between these systems and Agency-operated systems.

Yes

10.a(5) The Agency requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.a(6) The inventory of contractor systems is updated at least annually.

Yes

10.a(7) Systems that are owned or operated by contractors or entities, including Agency systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Comments: SSA had 11 contractor systems. We tested 4 systems and found one contractor system where SSA did not comply with the Federal requirements for contractor system oversight.

Section 11: SECURITY CAPITAL PLANNING

11.a. The Agency has established and maintains a security capital planning and investment program for information security. Although improvement opportunities may have been identified by the OIG, the program includes the following attributes:

11.a(1) Documented policies and procedures to address information security in the capital planning and investment control process.

Yes

11.a(2) Includes information security requirements as part of the capital planning and investment process.

Yes

11.a(3) Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.a(4) Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

11.a(5) Ensures that information security resources are available for expenditure as planned.

Yes

Background and Current Security Status

The *Federal Information Security Management Act of 2002* (FISMA) requires that agencies create protective environments for their information systems. It does so by creating a framework for annual information technology security reviews, vulnerability reporting, and remediation planning, implementation, evaluation, and documentation.[1] In Fiscal Year (FY) 2005, the Social Security Administration (SSA) resolved the long-standing internal controls reportable condition concerning its protection of information.[2] However, during the FY 2009 through 2011 financial statement audits, SSA's management of access to its systems was identified as a significant deficiency.[3] SSA continues to work with us and Grant Thornton LLP to further improve the security and the protection of information and information systems and resolve other issues observed during prior FISMA reviews.

This year, the Department of Homeland Security (DHS) prepared the FY 2011 Inspector General (IG) *Federal Information Security Management Act Reporting* metrics, and will oversee agencies' compliance with FISMA. DHS will also develop analyses for the Office of Management and Budget (OMB) to assist in the development of the FISMA annual report. However, OMB will be responsible for the submission of the annual FISMA report to Congress.[4]

The FY 2011 FISMA guidance, DHS Federal Information Security Memorandum 11-02, states that the goal for Federal information security in FY 2011 is to build a defensible Federal enterprise that enables agencies to harness technological innovation, while

---

[1] Pub. L. 107-347, Title III, Section 301, 44 U.S.C. § 3544(a)(1), (a)(2), and (b)(1).

[2] SSA, *FY 2005 Performance and Accountability Report,* p. 164.

[3] The definition of **a significant deficiency for financial statement internal control** is provided by the Statement on Auditing Standards Number 115 *Communicating Internal Control-Related Matters Identified in an Audit.* This Statement on Auditing Standards states a significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. OMB provides the definition of **a significant deficiency under FISMA**. DHS FISM 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* Frequently Asked Questions section, August 24, 2011, p. 8, defines a significant deficiency as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

[4] OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010.

protecting agency information and information systems.[5] To comply with the guidance, agencies must carry out the following three activities.[6]

1. *Monthly Data Feeds.* Each month, agencies must load data from their automated security management tools into DHS' CyberScope tool for a limited number of data elements. The shift from the once-a-year FISMA reporting process to a monthly reporting of key metrics through CyberScope allows security practitioners to make decisions using more information—delivered more quickly than ever before.

2. *Information Security Questions.* Agencies must answer a set of information security questions in CyberScope. These questions address areas of risk and are designed to assess the implementation of security capabilities and measure their effectiveness.

3. *CyberStat Review Sessions and Agency Interviews.* Through CyberStat, DHS cybersecurity experts engage with selected agencies to help them develop focused action plans for improving their information security postures. For those agencies not selected for a formal CyberStat review, a team of Government security specialists will conduct interviews focused on specific threats facing each agency as a consequence of its unique mission.

For FY 2011, IGs must assess their agencies' performance in 11 major FISMA programs specified by DHS using pre-established key attributes for each program.[7] IGs were also required to determine areas for significant improvement if any agency programs did not have these key attributes.[8] See details in Appendix B.

This report informs Congress and the public about SSA's information security performance and fulfills OMB's requirement under FISMA to submit an annual report to Congress. It provides the results of an assessment of SSA's information technology security strengths and weaknesses and a plan of action to improve performance. DHS requires that agencies use CyberScope to submit the annual FISMA report.

[5] DHS FISM 11-02, supra at p.1.

[6] Id. at pp.1-2.

[7] DHS, *FY 2011 Inspector General Federal Information Security Management Act Reporting, Version 1.0*, June 1, 2011.

[8] The DHS-specified attributes for each program and the significant improvement examples are posted on DHS's CyberScope Website. The agency Chief Information Officers and IGs all report through CyberScope.

Scope and Methodology

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Office of Inspector General (OIG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices, as well as a review of an appropriate subset of agency systems.[1] We contracted with Grant Thornton LLP (GT) to audit the Social Security Administration's (SSA) Fiscal Year (FY) 2011 financial statements. Because of the extensive internal control system work that is completed as part of that audit, our FISMA review requirements were incorporated into the GT financial statement audit contract. This evaluation included *Federal Information System Controls Audit Manual* level reviews of SSA's financial related information systems. GT performed an "agreed-upon procedures" engagement using FISMA; Department of Homeland Security Federal Information Security Memorandum 11-02, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; National Institute of Standards and Technology guidance; *Federal Information System Controls Audit Manual*; and other relevant security laws and regulations as a framework to complete the OIG-required review of SSA's information security program and practices and its information systems.

The results of our FISMA evaluation are based on our FY 2011 financial statement audit and working papers related to its agreed-upon procedures engagement as well as various audits and evaluations performed by this office and other entities. We also reviewed SSA's 2011 FISMA *Chief Information Officer Section Report*.

Our evaluation followed the Department of Homeland Security's FY 2011 FISMA guidance and focused on Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plans of Action and Milestones, Remote Access Management, Identity and Access Management, Continuous Monitoring Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

We performed field work at SSA facilities nationwide from March to October 2011. We considered the results of other OIG audits performed in FY 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.

[1] Pub. L. No. 107-347, Title III, section 301(b), § 3545 (a)(1), (a)(2), and (b)(1), 44 U.S.C § 3545 (a)(1), (a)(2), and (b)(1).

The Social Security Administration's Major Systems

	System	Acronym
	General Support Systems[1]	
1	Audit Trail System	ATS
2	Comprehensive Integrity Review Process	CIRP
3	Death Alert Control and Update System	DACUS
4	Debt Management System	DMS
5	Enterprise Wide Mainframe & Distributed Network Telecommunications Services System	EWANS
6	FALCON Data Entry System	FALCON
7	Human Resources Management Information System	HRMIS
8	Integrated Client Data Base System	ICDB
9	Integrated Disability Management System	IDMS
10	Quality System	QA
11	Security Management Access Control System	SMACS
12	Social Security Administration Online Accounting and Reporting System	SSOARS
13	Security Unified Measurement System	SUMS
	Major Applications[2]	
1	Electronic Disability	eDib
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR

[1] Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, Section A.2.c, defines a "general support system" or "system" as an interconnected set of information resources under the same direct management control which shares common functionality.

[2] Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, Section A.2.d, defines a "major application" as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

	System	Acronym
5	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Social Security Number Establishment and Correction System	SSNECS
8	Title II	T2

OIG Contacts and Staff Acknowledgments

OIG Contacts

Brian Karpe, Director, Information Technology Audit Division

Grace Chi, Acting Audit Manager

Acknowledgments

In addition to those named above:

Tina Nevels, Auditor

Michael Zimmerman, 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 Assistant at (410) 965-4518. Refer to Common Identification Number A-14-11-01134.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget

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, House of Representatives

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

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

Chairman and Ranking Minority Member, Committee on Commerce, Science and Transportation, U.S. Senate

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

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.