



SOCIAL SECURITY

The Commissioner

August 28, 2013

The Honorable Max Baucus
Chairman, Committee on Finance
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

We are providing you with our fiscal year (FY) 2012 Federal Information Security Management Act report as required by the Office of Management and Budget's (OMB) Memorandum 12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Our report 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). The OIG's report includes an independent evaluation of our information security program. We submitted these documents to OMB in November 2012.

I am pleased to report that of the 24 agencies required by the Chief Financial Officers Act of 1990 to perform this assessment, we ranked fourth. We have a score of 98 percent in our security compliance. I assure you that I will continue to enhance our programs to protect against threats to our information systems and sensitive information.

I hope you find the information helpful. I am also providing this information to the following Representatives: Becerra, Camp, Connolly, Cummings, DeLauro, Issa, Eddie Bernice Johnson, Sam Johnson, Kingston, Levin, Lowey, Mica, Rogers, and Smith. In addition, I am providing the information to the following Senators: Brown, Carper, Coburn, Harkin, Hatch, Mikulski, Moran, Rockefeller, Shelby, Thune, and Toomey.

If you have any questions, please have your staff contact Bill Zielinski, our Acting Chief Information Officer, at (410) 965-4380.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure



SOCIAL SECURITY
The Commissioner

August 28, 2013

The Honorable Dave Camp
Chairman, Committee on
Ways and Means
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We are providing you with our fiscal year (FY) 2012 Federal Information Security Management Act report as required by the Office of Management and Budget's (OMB) Memorandum 12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. Our report 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). The OIG's report includes an independent evaluation of our information security program. We submitted these documents to OMB in November 2012.

I am pleased to report that of the 24 agencies required by the Chief Financial Officers Act of 1990 to perform this assessment, we ranked fourth. We have a score of 98 percent in our security compliance. I assure you that I will continue to enhance our programs to protect against threats to our information systems and sensitive information.

I hope you find the information helpful. I am also providing this information to the following Representatives: Becerra, Connolly, Cummings, DeLauro, Issa, Eddie Bernice Johnson, Sam Johnson, Kingston, Levin, Lowey, Mica, Rogers, and Smith. In addition, I am providing the information to the following Senators: Baucus, Brown, Carper, Coburn, Harkin, Hatch, Mikulski, Moran, Rockefeller, Shelby, Thune, and Toomey.

If you have any questions, please have your staff contact Bill Zielinski, our Acting Chief Information Officer, at (410) 965-4380.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure



SOCIAL SECURITY

The Commissioner

November 15, 2012

The Honorable Jeffrey Zients
Acting Director, Office of Management
and Budget
725 17th Street, NW
Washington, D.C. 20503

Dear Mr. Zients,

As required by the Office of Management and Budget's (OMB) Memorandum 12-20 (M-12-20), *Fiscal Year (FY) 2012 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management*, we are submitting our FY 2012 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). The OIG's report includes an independent evaluation of our information security program and FISMA compliance.

In accordance with FISMA, we are reporting that the OIG cited a significant deficiency in our information security program for FY 2012 based upon the financial statement auditor's finding of a material weakness in our information systems controls. However, we do not agree that the auditor's findings rise to the level of a material weakness in our information systems controls. As we do with all auditor findings, we are pursuing a risk-based corrective action plan, and OIG's report documents our efforts to resolve the findings. We will continue to enhance our overall security program.

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

2012

Annual FISMA
Report

Social Security Administration

Section 1: System Inventory

- 1.1 For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low) in this question, provide the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below. (Organizations with below 5000 users may report as one unit.)
- 1.2 For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Organization operational, information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below.

Agency/ Component		1.1a Organization Operated Systems	1.1b Contractor Operated Systems	1.1c Systems (from 1.1a and 1.1b) with Security ATO	1.2a Systems utilizing cloud computing resources	1.2b Systems utilizing cloud computing resources (1.2a) with a Security Assessment and Authorization	1.2c Systems in 1.2a utilizing a FedRAMP authorized Cloud Service Provider
SSA	High	0	0	0	0	0	0
	Moderate	16	0	16	2	2	0
	Low	5	0	5	0	0	0
	Not Categorized	0	0	0	0	0	0
	Sub-Total	21	0	21	2	2	0
The SSA inventory process accounts for contractor/cloud systems by incorporating them into larger system authorization boundaries. These contractor/cloud components are documented accordingly in the applicable system security plans.							
Component Total	High	0	0	0	0	0	0
	Moderate	16	0	16	2	2	0
	Low	5	0	5	0	0	0
	Not Categorized	0	0	0	0	0	0
	Total	21	0	21	2	2	0

Section 2: Asset Management

- 2.0 Hardware Assets: Provide the total number of organization hardware assets connected to the organization's unclassified network(s).**
276165
- 2.1 Provide the number of assets in 2.0, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.**
276165
- 2.1a How often are these automated capabilities (device discovery processes) conducted on all assets connected to the organization's full network(s)? (frequency in days)**
15.0
- 2.1a(1) How much time does it take a device discovery tool to complete this process? (Duration in days; e.g. 10 days or 0.2 days)**
7.0
- 2.1b Provide the number of assets in 2.0, where all of the following information is collected: Network IP address, Machine Name, MAC Address (or other hardware identifier like serial number).**
276165
- 2.2 Provide the number of assets in 2.0, where the organization has an automated capability to determine whether the asset is authorized and to determine who manages it.**
0
- 2.3 Provide the number of assets in 2.0, where the organization has an automated capability to compare 2.1 and 2.2, to identify and remove (manually or through NAC, etc.) the unauthorized devices.**
0
- 2.3a For the assets in 2.3, how much time does it actually take to a) assign for management (authorize) or b) remove unauthorized devices once discovered with 95% confidence? (Duration in days; e.g. 10.00 days or 0.20 days)**
0.0
- 2.3b Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and mitigate unauthorized routes, including routes across air-gapped networks.**
0

Section 2: Asset Management

2.4 Software Assets: Can the organization track the installed operating system Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0?

Yes

2.4.a Can the organization track, (for each installed operating system Vendor, Product, Version, and patch-level combination in 2.4) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning?

No

2.4.a(1) Why not?

SSA does not currently have the capability to track this metric without scanning.

2.5 Does the Organization have a current list of the enterprise-wide COTS general purpose applications (e.g., Internet Explorer, Adobe, Java, MS Office, Oracle, SQL, etc.) installed on the assets in 2.0?

Yes

2.5a For each enterprise-wide COTS general purpose applications in 2.5, can the Organization report the number of assets in 2.0 on which it is installed by CPE in order to know the number of application vulnerabilities which are present without scanning?

No

2.5.a(1) Why not?

SSA does not currently have the capability to track this metric without scanning.

2.6 Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and block unauthorized software from executing, or where no such software exists for the device type.

0

Section 3: Configuration Management

3.1 For each operating system Vendor, Product, Version, and patch-level combination referenced in 2.4, report the following:

3.1a Whether an adequately secure configuration baseline has been defined.

Yes

Section 3: Configuration Management

- 3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).
250128
- 3.1c For what percentage of the applicable hardware assets (per question 2.0), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1a and provide visibility at the organization's enterprise level?
91
- 3.1d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions)
30.0
- 3.2 For each of the enterprise-wide COTS general purpose applications Vendor, Product, Version, and patch-level combination referenced in question 2.5., report:
- 3.2a Whether an adequately secure configuration baseline has been defined.
Yes
- 3.2b The number of hardware assets with this software (which are covered by this baseline, if it exists).
0
- 3.2c For what percentage of the applicable hardware assets, with each kind of software in 3.2, has an automated capability to identify configuration deviations from the approved defined baselines and provide visibility at the organization's enterprise level?
0
- 3.2d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions)
0.0
- 3.3 Report the number of hardware assets from 2.0 to which the FDCC/USGCB baseline applies.
139001

Section 3: Configuration Management

- 3.3a Report the number of CCEs in the FDCC/USGCB baselines where the organization has approved deviations from the FDCC/USGCB standard across the organization (or organizational sub-components). List those specific CCEs in the comment.**
300

Comments: SSA's comprehensive submission for metric 3.3a is contained within supplemental artifact "SSA_FY12_CCE_Deviations.pdf" (labeled as "Other" within CyberScope). The supplemental artifact contains a list of SSA's CCE deviations.

- 3.3b For each CCE in 3.3a, indicate in the comment the CCE and the number of assets in 2.1 to which the FDCC/USGCB standard applies, but has been relaxed (through an approved deviation) by the organization. Report the sum of these numbers (count of asset-CCE pairs that have been relaxed) in the response.**
21110130

Comments: The counts for devices in question 3.3 are centrally managed, general purpose desktops where policy is managed through GPOs. The deviations listed apply to those machines for their respective operating systems. SSA's comprehensive submission for metric 3.3b is contained within supplemental artifact "SSA_FY12_CCE_Deviations.pdf" (labeled as "Other" within CyberScope). The supplemental artifact identifies the count of asset-CCE pairs that have been relaxed by O/S type.

Section 4: Vulnerability and Weakness Management

- 4.1 Provide the number of hardware assets identified in section 2.0 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.**
150264

- 4.1.1 Provide the number of hardware assets identified in section 2.0 that were evaluated using tools to assess the security of the systems and that generated output compliant with each of the following:**

4.1.1a Common Vulnerabilities and Exposures (CVE)

150264

4.1.1b Common Vulnerability Scoring System (CVSS)

150264

Section 4: Vulnerability and Weakness Management

4.1.1c Open Vulnerability and Assessment Language (OVAL)

150264

- 4.2 National Vulnerability Database (NVD) and the Secure Content Automation Program (SCAP) are focused primarily on common COTS operating systems and applications, after they are released. However, COTS and non-COTS software need to be searched for weaknesses before release. It is often useful to check open-source software for weaknesses, if the developer has not thoroughly done so. What methods has your organization considered using to find, identify and assess weaknesses that may be in software that your organization develops and uses?

Section 4: Vulnerability and Weakness Management

	a. Have you considered using this tool?	b. Are you using this now?	c. Describe this method	d. Is this a viable solution?	What are the obstacles?
a. Identify Universe Enumeration					
Common Weakness Enumeration (CWE)	Yes	Yes	SSA acquired HP Fortify Static Code Analyzer tool that provides output compliant to CWE. The reports produced identify and rank security vulnerabilities.	Yes	There are no obstacles identified at this time.
Web scanners for web-based applications	Yes	Yes	SSA acquired HP WebInspect Dynamic scanning tool that provides output compliant to CWE. The reports produced identify and rank security vulnerabilities.	Yes	There are no obstacles identified at this time.
Common Attack Pattern Enumeration and Classification	No	No	N/A	No	Currently SSA has identified projects of higher priority. Other obstacles include a lack of resources and the need to change our established development procedures.

Section 4: Vulnerability and Weakness Management

b. Find Instances Tools and Languages					
Static Code Analysis Tools	Yes	Yes	SSA acquired the HP Fortify Static Code Analyzer and the Semantic Designs Quality Scanning tools which are used during the development phase of the software development life cycle.	Yes	There are no obstacles identified at this time.
Manual code reviews (especially for weaknesses not covered by the automated tools)	Yes	Yes	SSA performs manual code reviews during the development phase of the software development life cycle.	Yes	There are no obstacles identified at this time.
Dynamic Code Analysis Tools	Yes	Yes	SSA acquired the HP Fortify Static Code Analyzer and the Semantic Designs Quality Scanning tools which are used during the development phase of the software development life cycle.	Yes	There are no obstacles identified at this time.

Section 4: Vulnerability and Weakness Management

Web scanners for web-based applications	Yes	Yes	SSA acquired HP WebInspect which is used during validation testing to conduct dynamic scans and limited penetration testing of applications.	Yes	There are no obstacles identified at this time.
PEN testing for attack types not covered by the automated tools.	Yes	Yes	SSA enlists the services of external companies to perform penetration testing on critical applications.	Yes	There are no obstacles identified at this time.
c. Assess Importance					
Common Weakness Scoring System (CWSS)	Yes	Yes	The static and dynamic scanning tools acquired by SSA rely on the CWSS as well as other factors to determine the ranking of vulnerabilities.	Yes	There are no obstacles identified at this time.

Section 4: Vulnerability and Weakness Management

- 4.2d List any other viable methods your organization has considered using to find, identify, and assess weaknesses that may be in software that your organization develops and uses?

Comments: SSA also employs code quality scanners and builds reusable Enterprise Architecture (EA) approved frameworks.

Method Type	Tool Name	a. Have you considered using this method?	b. Are you using this now?	c. Describe this method	d. What are the Obstacles?
None Identified					

- 4.3 For what percentage of information systems does the organization:

Comments: SSA does not currently collect this data.

Impact Level	For systems in development and/or maintenance:		For systems in production:	
	Use methods described in section 4.2 to identify and fix instances of common weaknesses, prior to placing that version of the code into production?	Can you find SCAP compliant tools and good SCAP content?	Report on configuration and vulnerability levels for hardware assets supporting those systems, giving application owners an assessment of risk inherited from the general support system (network)?	Can you find SCAP compliant tools and good SCAP content?
High	0%	No	0%	No
Moderate	0%	No	0%	No
Low	0%	No	0%	No

Section 5: Identity and Access Management

- 5.1 What is the number of Organization unprivileged network user accounts? (Exclude privileged network user accounts and non-user accounts)

76833

Section 5: Identity and Access Management

5.2 How many unprivileged network user accounts are configured to:

Comments: SSA requires the use of either a User-ID and Password or Two factor authentication using a PIV card.

	Require the form of identification listed on the left?	Allow, but not require, the form of identification listed on the left?
a. User-ID and Password	0	76833
b. Two factor-PIV Card	0	76833
c. Other two factor authentication	0	0

5.3 What is the number of Organization privileged network user accounts? (Exclude non-user accounts and unprivileged network user accounts)

8739

5.4 How many privileged network user accounts are configured to:

Comments: SSA requires the use of either a User-ID and Password or Two factor authentication using a PIV card.

	Require the form of identification listed on the left?	Allow, but not require, the form of identification listed on the left?
a. User-ID and Password	0	8739
b. Two factor-PIV Card	0	8739
c. Other two factor authentication	0	0

5.5 What is the number of Organization unprivileged (high and moderate impact) application user accounts? (Exclude privileged application user accounts and non-user accounts)

N/A

Comments: All SSA users must authenticate at the network level to access agency applications.

5.6 How many unprivileged application user accounts are configured to:

	Require the form of identification listed on the left?	Allow, but not require, the form of identification listed on the left?
a. User-ID and Password	X	X
b. Two factor-PIV Card	X	X
c. Other two factor authentication	X	X

Section 5: Identity and Access Management

5.7 What is the number of Organization privileged application user accounts? (Exclude non-user accounts and unprivileged application user accounts)

N/A

5.8 How many privileged application user accounts are configured to:

	Require the form of identification listed on the left?	Allow, but not require, the form of identification listed on the left?
a. User-ID and Password	X	X
b. Two factor-PIV Card	X	X
c. Other two factor authentication	X	X

5.9 Provide the percent of privileged network users whose privileges were reviewed this year for:

5.9a Privileges on that account reconciled with work requirements

100%

Comments: This exercise is ongoing.

5.9b Adequate separation of duties considering aggregated privileges on all accounts for the same person (user)

100%

Comments: This exercise is ongoing.

5.9c Provide the percent of privileged network users whose privileges were adjusted or terminated after being reviewed this year.

0%

Comments: SSA does not collect this information at this time but will begin doing so in FY13.

5.10 Describe any best practices your Organization has developed in any of the following areas which are generally difficult in Federal Organizations.

5.10a Methods to identify accounts that actually have elevated privileges even though not intended or indicated by the account name.

Elevated privileges can be determined by a combination of classification code assigned to each account on the mainframe and group membership in Active Directory. SSA centrally manages membership for restricted administrator groups. If an unauthorized attempt is made to add an account to a privileged group, the change is disallowed, an event is recorded by an Active Directory auditing tool and an alert is sent to the security administrators

Section 5: Identity and Access Management

- 5.10b** Methods used to accurately and automatically identify all of the accounts assigned to the same person. Multiple accounts assigned to the same person are identified by being associated with the user's SSN.
- 5.10c** Methods used to identify all account holders who have departed location or service and should have their accounts disabled and removed, especially if your method covers all account holders (your organization's direct hire employees, institutional contractors, persons detailed to your organization from others, locally engaged staff overseas, etc.) by the same method. Employee status is maintained by Human Resources. If the status indicates that an employee is no longer with SSA (retirement, removal, etc.) a daily process records the account and, if this status remains for a two week period, the account is deleted from Active Directory. In addition, an automatic disabling process identifies all user accounts where the password has not been changed in over 60 days. If the condition remains for over two weeks, the account is disabled. Once disabled, an automated account deletion process runs daily and records accounts that have not been logged into and/or changed the password in 365 days. If this condition remains for a two week period, the account is then deleted. Accounts disabled/ deleted by these processes are captured and monitored using an Active Directory auditing tool.

Section 6: Data Protection

- 6.1** Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table.

Comments:

SSA does not track USB connected devices at this time; however, the agency has employed controls that ensure any data stored on these devices is encrypted per US Government standards. Other Mobile devices: UbiDuo (device for the deaf and hard of hearing) - 1392 Braille Notetakers - 176

Mobile Assets Types (each asset should be recorded no more than once in each column)	Estimated number of mobile hardware assets of the types indicated in each row	Estimated number assets from column a with adequate encryption of data on the device.
Laptop Computers, Netbooks and Tablet-Type Computers	13982	13982
Personal Digital Assistant	0	0
BlackBerries and Other Smartphones	4300	4300
USB connected devices (e.g., Flashdrives and Removable Hard Drives)	0	0
Other mobile hardware assets (describe types in comments field)	1568	0

Section 6: Data Protection

- 6.2 Provide the percentage of Organization email traffic on systems that implement FIPS 140-2 compliant 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, OpenPGP, or PKI.
100
- 6.3 Select the description that best describes your Organization's PKI Certificate Authority, and respond with the number of that option.
The organization:
3. Receives PKI support from a Federal or commercial Shared Service Provider, but which is responsible for some portion of the PKI service.
- 6.4 What percentage of the applicable Security Controls from NIST SP 800-53A (profiled by FPKIPA) does the PKI Certificate Authority and related PKI Infrastructure your organization uses adequately satisfy?

100

Comments: SSA uses the Department of Treasury PKI.

Section 7: Boundary Protection

- 7.1 Provide the percentage of the required TIC 1.0 Capabilities that are implemented.
100%
- 7.1a Provide the percentage of TIC 2.0 Capabilities that are implemented.
91%
- 7.2 Provide the percentage of TICs with operational NCPS (Einstein) deployment.
100%
- 7.2a Provide the percentage of TICs with operational Einstein 2 deployment.
100%
- 7.2b Provide the percentage of TICs with operational Einstein 3 deployment.
0%
- 7.3 Provide the percentage of external network traffic to/from the organization's networks passing through a TIC/MTIPS.
100%

Section 7: Boundary Protection

- 7.4 Provide the percentage of external network/application interconnections to/from the organization's networks passing through a TIC/MTIPS.
100%
- 7.5 Provide the percentage of Organization email systems that implement sender verification (anti-spoofing) technologies when sending messages.
100%
- 7.6 Provide the percentage of Organization email systems that check sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network.
100%
- 7.7 Provide the estimated percent of incoming email traffic (measured in messages) where the link/attachment is executed/opened in a sandbox/virtual environment in-line to ascertain whether or not it is malicious, and quarantined as appropriate, before it can be opened by the recipient. (Note: If you consider this to be infeasible, please explain why in the comments.)
0%
- 7.8 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts scheduled scans for unauthorized wireless access points (WAP) connected to an Organizational network.
0.25
- 7.8a Provide the percentage of hardware assets, identified in section 2.0 (Asset Management), which are in facilities where WAP scans are conducted.
0%
- 7.9 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts unscheduled scans for unauthorized wireless access points.
180.0
- 7.10 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization maps their cyber perimeter (e.g. publically accessible systems, externally visible systems and devices) for each network.
30.0

Section 7: Boundary Protection

- 7.11 Provide the percent of client browsers that are required to run only in a virtual environment.
0
- 7.12 What percentage of network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities and are adequately configured as intended, such as to adequately protect security?
100%
- 7.13 Provide the number of cloud systems from question 1.2a where traffic entering and exiting the cloud:
- 7.13a does not pass through a TIC?
0
- 7.13b are not required to pass through a TIC?
0
- 7.14 Provide the number of networks with DLP/DRM at the gateway to capture outbound data leakage (e.g., PII).
1

Section 8: Incident Management

- 8.1 What is the number of Organization hardware assets (from question 2.0) on networks on which controlled network penetration testing was performed in the reporting period?

1

Comments:

SSA conducted one penetration testing exercise on a high-priority, public-facing system that facilitates access by members of the public to personally identifiable information. This system is comprised of numerous components.

- 8.1a Percentage of applicable events detected by NOC/SOC during the penetration test.
0%
- 8.1b Median time to detection of applicable events. (Time in days and fractions of days. See General Instructions.)
0.0

Section 8: Incident Management

8.2 During FY12, for what percentage of US-CERT Security Awareness Reports (SARs), or the equivalent for DoD, has the organization adequately remediated or acted upon the actionable recommendations contained in the report? Please use the Comment function to comment on how the SAR process is meeting its goal and/or could be improved.

100%

Comments: The SAR process tends to lag behind other sources of the same information.

8.3 Provide the percentage of incidents that have been detected and attributed to successful phishing attacks. Please provide a Comment to describe any innovative and effective ways your organization has found to address these attacks.

0%

Comments: SSA acquired the Wombat Anti-phishing Awareness Tool to provide proactive security training, awareness and education for SSA employees and contractors on how to recognize and avoid threats caused by email phishing. In addition, SSA's enterprise security tools are used to scan the agency's networks and information systems for threats such as malware that are the result of such attacks.

Section 9: Training and Education

9.1 Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually).

80068

9.1a Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access, or within an organizationally defined time limit, providing adequate security, after being granted access.

100%

9.2 To what extent were users given cybersecurity awareness training content more frequently than annually (content could include a single question or tip of the day)?

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

9.2a Provide the average frequency in days between content provision. See General Instructions.

120.0

Section 9: Training and Education

- 9.2b Provide the percentage of this additional content that addresses emerging threats that were not previously covered in the annual training?
100
- 9.2c At what frequency is security awareness training content (that is provided to users) updated by the Organization or training provider? (Average frequency in days during FY2012. See General Instructions.)
120.0
- 9.2d Provide the total number of Organization-sponsored emerging threat exercises (such as phishing) designed to increase cybersecurity awareness and/or to measure the effectiveness of cybersecurity awareness training in molding behavior.
2
- 9.2e Provide the percentage of exercises in 9.2d where either no problems were found, or in which the problems were addressed through appropriate training within three months.
100
- 9.3 Provide the number of the Organization's network users and other staff with significant security responsibilities.
381
- 9.3a Provide the number of people in 9.3 that have been given training to perform their significant cybersecurity responsibilities at an organizationally defined frequency that has been determined to provide adequate security.
381
- 9.3b Provide the longest organizationally defined frequency that has been determined to provide adequate security for any role among those included in significant security responsibilities. (Days between training events. See general instructions)
365.0
- 9.3c At what frequency is training to perform their significant cybersecurity responsibilities updated by the Organization or training provider? (Average frequency in days across roles during FY2012. See General Instructions.)
365.0

Section 10: Remote Access

Section 10: Remote Access

10.1 Provide the estimated total number of annual remote connections the Organization provides to allow users to connect to near-full access to the Organization's normal desktop LAN/WAN resources/services.

259000

10.1a For those connections counted above in 10.1, provide the estimated number of those connections that:

Comments:

SSA does not scan remote hosts for malware; however, hosts are scanned for compliance with the approved security configuration prior to being granted access. In the event that a host is not configured appropriately, it is quarantined until it has been updated.

For each type of connection listed below, please provide the number of connections that use the authentication method listed to the right.	ONLY User-ID and Password	ONLY Two factor-PIV	ONLY Other two factor authentication	Only one other (please describe in the comments)	Connections that may have been authenticated multiple ways
Type of Connection					
Dial-Up	0	0	0	0	0
Virtual Private Network (not clientless)	0	244541	14459	0	0
Virtual Private Network (clientless) including SSL, TLS, etc.	0	0	0	0	0
Citrix	0	0	0	0	0
Other	0	0	0	0	0

10.1b For those connections counted above in 10.1a column e), provide the estimated number of those connections that:

For each type of connection listed below, please provide the number of connections that use the authentication method listed to the right.	User-ID and Password	Two factor-PIV Card	Other two factor authentication	Other(s). (Please describe in the comments.)
Type of Connection				
Dial-Up	0	0	0	0
Virtual Private Network (not clientless)	0	0	0	0
Virtual Private Network (clientless) including SSL, TLS, etc.	0	0	0	0
Citrix	0	0	0	0
Other	0	0	0	0

Section 10: Remote Access

- 10.1c** For those connections counted above in 10.1, provide the estimated percentage of those connections that:
Utilize FIPS 140-2 validated cryptographic modules.
100
- Prohibit split tunneling and/or dual-connected remote hosts where the laptop has two active connections.
100
- Are configured in accordance with OMB M-07-16, to time-out after 30 minutes of inactivity (or less) requiring re-authentication to reestablish session.
100
- Scan for malware upon connection.
0
- Require Government Furnished Equipment (GFE).
100
- Assess and correct system configuration upon connection of GFE.
100

Section 11: Network Security Protocols

- 11.1** Provide the number of public facing domain names (second-level, e.g. www.dhs.gov). (You should exclude domain names which host only FIPS 199 low-impact information on ISPs.)
7
- 11.1a** Provide the number of DNS names from 11.1, signed using DNSSEC.
3
- 11.1b** Provide the percentage of the second-level DNS names from 11.1 and their sub-domains for which all domain names at and under the second level are signed.
100%

Section 11: Network Security Protocols

11.2 Provide the percentage of public facing servers that use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and ISP resources from the numerator and denominator unless they require IPv6 to perform their business function.)

95%

Inspector General

Section Report

2012

Annual FISMA
Report

Social Security Administration

Section 1: Continuous Monitoring Management

- 1.1 Has the Organization 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

- 1.1.1 Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7)

Yes

- 1.1.2 Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G)

Yes

- 1.1.3 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A)

Yes

Comments:

To date, SSA had not fully implemented its continuous monitoring program. For example, the Agency had not developed risk models for some of the hardware and software connected to its network. Therefore, the Agency did not continually monitor these operating system platforms and applications.

- 1.1.4 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 (NIST 800-53, NIST 800-53A)

Yes

Comments:

SSA's current continuous monitoring could not provide a comprehensive view and near real-time information of the enterprise.

- 1.2 Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above

See Comments

Comments:

SSA did have a continuous monitoring strategy, but it had not been fully implemented. For example, SSA had identified, evaluated, and implemented, some continuous monitoring tools for its operating environment. However, the Agency needed additional time to ensure the continuous monitoring tools were fully operable within its information system environment. Consequently, SSA's continuous monitoring program could not provide a comprehensive view and near real-time information of the enterprise. Weaknesses identified in this area contributed to a financial statement audit material weakness identified by Grant Thornton, LLP (GT). Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 2: Configuration Management

2.1 Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

2.1.1 Documented policies and procedures for configuration management

Yes

2.1.2 Standard baseline configurations defined

Yes

Comments: The Agency had established baseline configurations for many, but not all, computer platforms.

2.1.3 Assessing for compliance with baseline configurations

Yes

Comments: We identified security weaknesses in the configuration settings of some SSA computer platforms. Internal penetration testers were able to obtain security information and personally identifiable information because some of SSA's systems were misconfigured. SSA had taken corrective action to address these issues.

2.1.4 Process for timely, as specified in Organization policy or standards, remediation of scan result deviations

Yes

2.1.5 For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented

Yes

2.1.6 Documented proposed or actual changes to hardware and software configurations

Yes

Comments: SSA monitored the hardware devices connected to its network to determine whether they complied with approved risk models and configuration settings. However, the Agency did not conduct impact assessments to determine the security implications for system changes. In addition, management did not have a formally documented process to periodically review the privileged programs added to the Agency's mainframe environment to ensure that all privileged programs are approved, cannot be improperly modified, and are safe. We also identified discrepancies in the approval and documentation of changes to SSA applications.

Section 2: Configuration Management

2.1.7 Process for timely and secure installation of software patches

Yes

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2)

No

Comments:

The Agency had implemented scanning procedures for some, but not all, platforms. SSA did not have a formal process in place for managing or obtaining a comprehensive list of approved software for all devices. However, the Agency had made efforts to develop this process.

2.1.9 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)

Yes

Comments:

Annual vulnerability scans and penetration testing have consistently identified security weaknesses. However, some security weaknesses were fully or partially remediated during the audit period. Since the Agency does not have risk models for all computer platforms, some configuration-related vulnerabilities went unidentified.

2.1.10 Patch management process is fully developed, as specified in Organization policy or standards. (NIST 800-53: CM-3, SI-2)

Yes

2.2 Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.

See Comments

Comments:

Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 3: Identity and Access Management

3.1 Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

Yes

Section 3: Identity and Access Management

3.1.1 Documented policies and procedures for account and identity management (NIST 800-53: AC-1)

Yes

3.1.2 Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)

Yes

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

Yes

Comments:

We identified programmers with access to production data that bypassed SSA's process to monitor and limit such access.

3.1.4 If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate (NIST 800-53, IA-2)

Yes

3.1.5 Organization has adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)

Yes

3.1.6 Ensures that the users are granted access based on needs and separation of duties principles

Yes

Comments:

Although SSA had an extensive access control program, internal penetration testers were able to take control of SSA's Windows network. Testing also identified personnel with inappropriate access and programmers with access to production data that bypassed SSA's process to monitor and limit such access. The Agency had not consistently implemented policies and procedures to periodically reassess the content of security access profiles. SSA was working to improve its profile and access recertification program and planned for a full implementation in Fiscal Year (FY) 2013.

3.1.7 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)

Yes

Comments:

Although SSA scanned its network to identify hardware devices connected to it, the Agency had been unable to categorize all hardware devices and their associated operating systems connected to its network. Further, SSA did not have an automated capability to determine whether hardware devices connected to its network were authorized.

Section 3: Identity and Access Management

3.1.8 Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)

Yes

3.1.9 Ensures that accounts are terminated or deactivated once access is no longer required

Yes

Comments:

Although SSA had policies and procedures to terminate access when it is no longer needed, we identified instances where physical and logical access was not removed timely.

3.1.10 Identifies and controls use of shared accounts

Yes

3.2 Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.

See Comments

Comments:

Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 4: Incident Response and Reporting

4.1 Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

4.1.1 Documented policies and procedures for detecting, responding to and reporting incidents (NIST 800-53: IR-1)

Yes

4.1.2 Comprehensive analysis, validation and documentation of incidents

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

Section 4: Incident Response and Reporting

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)

Yes

Comments:

SSA reported incidents to OIG in a timely manner. The Agency did not have an established timeframe for reporting incidents to external law enforcement or the Federal Protective Services. SSA identified incidents reported to external law enforcement or the Federal Protective Services; however, the Agency did not provide police reports for sampled incidents.

4.1.5 Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable

Yes

4.1.7 Is capable of correlating incidents

Yes

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.2 Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.

N/A

Section 5: Risk Management

5.1 Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

5.1.1 Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process

Yes

Section 5: Risk Management

5.1.2 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

Comments:

SSA had a decentralized governance structure for IT security. This resulted in a system misconfiguration going undetected, enabling GT to obtain security and personally identifiable information. In addition, SSA lacked a centralized process to authorize hardware devices before they were connected to the Agency's network.

5.1.3 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

5.1.4 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

5.1.5 Categorizes information systems in accordance with government policies

Yes

5.1.6 Selects an appropriately tailored set of baseline security controls

Yes

5.1.7 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

5.1.8 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

Comments:

Financial statement audit testing found that SSA's vulnerability testing was insufficient.

5.1.9 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

Section 5: Risk Management

5.1.10 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

Comments:

SSA performed security authorizations and annual security testing of selected controls. However, SSA's continuous monitoring program was not fully implemented. See comment for Metric 1.2.

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

Yes

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

Yes

5.1.13 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

5.1.14 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37)

Yes

5.1.15 Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

Yes

5.2 Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

See Comments

Comments:

Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 6: Security Training

Section 6: Security Training

6.1 Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

6.1.1 Documented policies and procedures for security awareness training (NIST 800-53: AT-1)

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities

Yes

6.1.3 Security training content based on the organization and roles, as specified in Organization policy or standards

Yes

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

Yes

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training

Yes

6.1.6 Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53).

Yes

6.2 Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.

N/A

Section 7: Plan Of Action & Milestones (POA&M)

7.1 Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.1.1 Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation

Yes

Comments: SSA's policy needed to be updated to reflect the current tools used to monitor and track security weaknesses.

7.1.2 Tracks, prioritizes and remediates weaknesses

Yes

Comments: We found some IT security risks that were tracked, but not prioritized.

7.1.3 Ensures remediation plans are effective for correcting weaknesses

Yes

7.1.4 Establishes and adheres to milestone remediation dates

Yes

Comments: We noted several POA&Ms that did not include a scheduled completion date.

7.1.5 Ensures resources are provided for correcting weaknesses

Yes

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25)

Yes

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25)

Yes

7.1.8 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 (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25)

Yes

7.2 Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.

N/A

Section 8: Remote Access Management

Section 8: Remote Access Management

8.1 Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17)

Yes

8.1.2 Protects against unauthorized connections or subversion of authorized connections.

Yes

8.1.3 Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1)

Yes

8.1.4 Telecommuting policy is fully developed (NIST 800-46, Section 5.1)

Yes

Comments: SSA's revised telework policy was in draft form, pending the resolution of administrative matters.

8.1.5 If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3)

Yes

8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms

Yes

8.1.7 Defines and implements encryption requirements for information transmitted across public networks

Yes

8.1.8 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

Comments: SSA exceeded best practice since its sessions time-out after 15 minutes of inactivity.

Section 8: Remote Access Management

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines)

Yes

8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53, PL-4)

Yes

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6)

Yes

8.2 Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.

N/A

Section 9: Contingency Planning

9.1 Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1)

Yes

9.1.2 The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34)

Yes

9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures (NIST SP 800-34)

Yes

9.1.4 Testing of system specific contingency plans

Yes

Comments:

The Agency did not conduct contingency plan testing for 2 of the 21 major systems/applications. For one of the applications, the application owners were not aware of the annual testing requirement. For the other application, the application owners were working with the appropriate subject matter experts to integrate their application into SSA's disaster recovery exercise.

Section 9: Contingency Planning

- 9.1.5 The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)
Yes
- 9.1.6 Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53)
Yes
- 9.1.7 Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans
Yes
- 9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34)
Yes
- 9.1.9 Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53)
Yes
- 9.1.10 Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)
Yes
- 9.1.11 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53)
Yes
- 9.1.12 Contingency planning that consider supply chain threats
Yes

Comments:

SSA's two data centers will back up each other. SSA considered supply chain threats for one data center, but not the other.

- 9.2 Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.

N/A

Section 10: Contractor Systems

Section 10: Contractor Systems

10.1 Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

Yes

10.1.1 Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

Yes

10.1.2 The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines

Yes

Comments:

For 12 of 17 contractor systems identified by our testing, SSA either performed a security authorization or obtained documentation of the systems' compliance with Federal security guidelines. Three of the contractor systems were operated or owned by other Federal or State agencies. One was operated by a contractor whose services were used by many Federal agencies. SSA believed it was not responsible for performing a security authorization of this contractor system. The remaining contractor system was a Website, located in a public cloud, but did not have the proper security authorization. However, the Website contained non-sensitive, public information, and a link that redirected users to SSA's secure Website to report fraud allegations.

10.1.3 A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud

No

Comments:

We found seven contractor systems that SSA had not identified on its inventory list.

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5)

Yes

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

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

Section 10: Contractor Systems

10.1.7 Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines

Yes

Comments: See comments for Metric 10.1.2.

10.2 Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.

See Comments

Comments: We found some IT-related contracts did not contain the proper FISMA security clause requirements.

Section 11: Security Capital Planning

11.1 Has the Organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process

Yes

11.1.2 Includes information security requirements as part of the capital planning and investment process

Yes

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2)

Yes

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3)

Yes

Comments: We identified inconsistencies in the supporting documents for some line items in Exhibit 53B. For example, some Exhibit 53B numbers were based on budget estimates rather than budget decisions.

11.1.5 Ensures that information security resources are available for expenditure as planned

Yes

Section 11: Security Capital Planning

11.2 Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

N/A

Senior Agency Official For Privacy

Section Report

2012
Annual
FISMA

Social Security Administration

Question 1: Information Security Systems

		1a. Number of Federal systems that contain personal information in an identifiable form			1b. Number of systems in column a. for which a Privacy Impact Assessment (PIA) is required under the E-Government Act			1c. Number of systems in column b. covered by a current PIA				1d. Number of systems in column a. for which a System of Records Notice (SORN) is required under the Privacy Act			1e. Number of systems in column d. for which a current SORN has been published in the Federal Register			
Agency/Component	Submission Status	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	Submitted to Agency	21	0	21	18	0	18	18	0	18	100%	21	0	21	21	0	21	100%
Agency Totals		21	0	21	18	0	18	18	0	18	100%	21	0	21	21	0	21	100%

Section 2: PIAs and SORNs

- 2a Provide the URL of the centrally located page on the agency web site that provides working links to agency PIAs (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 (N/A if not applicable).
<http://www.socialsecurity.gov/foia/bluebook/toc.htm>

Section 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:

As documented in our regulations (20 C.F.R. § 401.30(e)), the SAOP assumes responsibility and accountability for ensuring the agency's implementation of information privacy protections, as well as agency compliance with federal laws, regulations, and policies relating to the privacy of information. Our Administrative Instructions Manual System (AIMS) (Chapter 15.01.04) further defines these responsibilities. The Office of Privacy and Disclosure (OPD), which the SAOP oversees, implements agency privacy policies and procedures. We participated in the agency's PII Breach Response Group and the E-Government Steering Committee to ensure privacy compliance. We reviewed, wrote, and amended Privacy Act Statements, SORNs, Privacy Threshold Analyses (PTA), PIAs, and the PII clauses found in our contracts. We maintain and annually review the disclosure program instructions section of the agency's internal Program Operations Manual System (POMS) to ensure privacy compliance.

Section 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 legislative initiatives involving new privacy policy, as well as requests for testimony and comments arising under OMB Circular A-19. As indicated in our regulations (20 C.F.R. § 401.30(e)), the SAOP has a central role in the agency's development and evaluation of legislative, regulatory, and other policy proposals which might implicate information privacy issues. For example, in FY 2012, the SAOP reviewed the Cybersecurity Act of 2012, the Improper Payments and Elimination and Recovery Act of 2012, and proposed legislative changes to the Internal Revenue Code of 1986 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, under 20 C.F.R. § 401.30, approves PIAs assessing the impact of technology on protecting the privacy of personal information and ensures privacy principles are integrated into all aspects of technology systems. Our integral review occurs early in the System Development Lifecycle (SDLC) via the Control, Audit, Security, and Privacy Certification checklist. We use our PTA process to assess privacy risks in systems or applications and to determine if a PIA or SORN is required. We also approve Project Scope Agreements and Business Process Descriptions associated with the system or application. Additionally, we collaborated with the Office of Systems to implement data loss prevention technology to mitigate the risk of PII disclosure via our communications systems. We also participated in workgroups to assess the technological impact of social media and other emerging technologies, such as an internal social media pilot and a mobile application for wage reporting.

Section 4: Privacy Training

Section 4: Privacy Training

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:

Our regulations (20 C.F.R. § 401.30(e)) provide that the SAOP ensure that employees and contractors receive training and education regarding privacy laws, regulations, policies, and procedures governing the agency's handling of personal information. We provide employees privacy education resources, and employees annually sign a sanctions document acknowledging their understanding of the penalties for misusing protected information. We also issue documentation to staff on safeguarding PII and adherence to the Privacy Act and other provisions. Our POMS, Chapter GN 033, contains instructions that apply to the disclosure of personal information in our records. In 2012, we devoted significant time and resources hosting privacy education and awareness activities. On National Data Privacy Day, we featured discussions on the use of social media and protecting PII. We also created a Video on Demand (VOD) this year to reach our employees not located within the local commuting area.

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 specialized training on the Privacy Act, and related privacy regulations, policies, and procedures. Employees have access to four specific VODs on protecting and safeguarding PII. In FY 2012, we continued our practice of training systems development staff on the importance of privacy and privacy risk assessment via the SDLC Configuration Control Board (CCB). By participating in the SDLC CCB, we review any proposed changes to lifecycle roles, activities, or work products that affect the administration of personal information and educate members on the importance of these activities. 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.

Section 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

Section 5: PIA and Web Privacy Policies and Processes

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:

Under our PTA process, we document our privacy analysis of new or modified technology and business processes. The agency's Project Resource Guide establishes our PTA process. We work with stakeholders on their systems, and via the PTA, analyze the need for a PIA or the modification of an existing PIA because of new systems or changes to existing systems. Our PIA process is established in our regulations (C.F.R. § 401.30(f)) and includes review and approval by multiple levels of management and involves the system owner and IT staff. Our PTA and PIA processes ensure that the appropriate standards for PIAs are met in accordance with OMB M-03-22 and § 208 of the E-Government 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

Section 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:

Our AIMS (Chapter 15.01.05) requires that we ensure compliance with rules and requirements concerning the protection of PII when making information available through our websites. In FY 2012, we acquired content-aware compliance software to examine our webpages. We review each website quarterly to ensure compliance with the Privacy Act and agency privacy policies, as well as the Children’s Online Privacy Protection Act (COPPA), the Gramm-Leach Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). We also scan our websites for Platform for Performance (P3P) requirements, collection of PII, and privacy vulnerabilities associated with on-line collection of PII. This software allows us to detect and eliminate web-tracking devices such as web beacons and unauthorized cookies.

Section 6: Conduct of 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	Y	Y	Y	3	193	Y	X	X	102	88	49	X
TOTAL				3	193				102	88	49	

Section 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.

0

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.

5

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

0

Section 8: Policy Compliance Review

Section 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:

As noted in our response to Question 3a, the SAOP is responsible for ensuring the agency's compliance with federal laws, regulations, and policies relating to the privacy of information. We have a mature Systems Process Improvement program that describes best practices for software development and implements standard processes and procedures for ensuring compliance. We integrate our Enterprise Architecture activities and our governance practices throughout our SDLC. A typical new software release takes six months from conclusion of the planning and analysis to production. We are involved during the planning and analysis stage, and thus are able to conduct and document our initial privacy assessment early in the SDLC.

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

Yes

Comments:

Our SDLC includes independent validation testing; independent integration and environmental testing; independent usability testing; user acceptance testing; and project scope agreements with all stakeholders. We use appropriate corrective actions during each phase of testing.

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

Yes

Comments:

During FY 2012, we launched content-aware compliance software and a data loss prevention tool to better identify any risks associated with our protection of personal information.

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

Yes

Comments:

Although we are not subject to section 522 of the Consolidated Appropriations Act of 2005, we work closely with the Inspector General on a variety of privacy issues.

Section 9: SAOP Advice and Guidance

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.

Section 9: SAOP Advice and Guidance

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

Yes

Comments:

The SAOP, through OPD, develops and interprets SSA policy governing the collection, use, maintenance, and disclosure of PII contained in SSA records in accordance with the privacy statutes and regulations. We developed policies to cover the growing use of social media and mobile technologies. The SAOP, in conjunction with other agency components, coordinated our FY 2012 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 PTA process that helps us determine whether a new or amended SORN or PIA is required for a system or application.

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, including targeted training on our policies and procedures. 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 participate on interagency committees and workgroups dedicated to privacy best practices and policies.

Section 9: SAOP Advice and Guidance

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

Yes

Comments:

Under the leadership of the SAOP, we provide comprehensive privacy training to our employees. Our POMS, Chapter GN 033, contains specific policy instructions that apply to the disclosure of personal information in our records. Also refer to our responses to questions 4a and 4b, above.

Section 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:

As previously reported in FY 2011, 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-10-22, Guidance for Online Use of Web Measurement and Customization 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:

Under the guidelines established by OMB M-10-22, stake-holding components review new uses of the technology as they are proposed. The review includes legal, privacy, and security compliance. We also review compliance with OMB's guidelines on an annual basis and did not identify any issues during our FY 2012 annual review.

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

Yes

Comments:

We performed the activities described in response to question 10b to ensure that we comply with OMB Memorandum M-10-22. We also continue to develop agency-wide guidance on emerging technologies and participate on interagency workgroups to share policies and strategies.

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.gov/privacy.html>.

FY 2012 FISMA

Senior Agency Official for Privacy Report

Update on Agency Efforts to Eliminate

Unnecessary Use of Social Security Numbers (SSN)

The Social Security Administration (SSA) recognizes the importance of eliminating the unnecessary use of SSNs. First introduced as a means of tracking contributions to the Social Security retirement system, the SSN is critical to the implementation of SSA's programs, and consequently is a necessary element in many of our information systems. Nevertheless, we continue to reduce our use of SSNs for non-program related purposes. Even where we need the SSN for program administration, we have reduced its use. We have continued to:

- Limit the use of the SSN in systems applications that do not require its use for every transaction. For example, applications that link to financial institutions may require the SSN for initial logon, but thereafter we use an account number or some other form of identification or authentication to reduce the use and transmission of SSNs.
- Review systems and applications that are being developed or revised. The Privacy Threshold Analysis portion of the systems development lifecycle ensures that we review any proposed new or revised collection of personally identifiable information and determine whether collection of an SSN is necessary to the operation of that system or application.
- Play a key role in limiting the further disclosure of SSNs once they are issued for enumeration purposes. We have removed the SSN from certain notices sent to the public. In addition, we review all requests for disclosure of an SSN to ensure that the disclosure is compatible with the original program purpose for which the SSN was collected and is otherwise in accordance with laws and policies limiting its disclosure.
- Review the need for collecting SSNs and eliminate the use of SSNs when their use is unnecessary for non-program purposes such as human resources. For example, we previously used SSNs to track our employees' training. We no longer collect SSNs for this purpose.



SOCIAL SECURITY

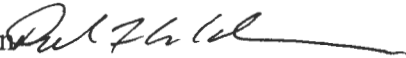
MEMORANDUM

Date: April 18, 2012

Refer To:

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 (OMB) Memorandum M-07-16 Requirement to Review and Reduce Agency Holdings of Personally Identifiable Information (PII) - 2012 Annual Review - Notice of Completion--INFORMATION

As you know, the Office of Management and Budget requires us to review our current holdings of all PII. This requirement ensures that our PII holdings are accurate, relevant, timely, and complete, and reduces them to the minimum necessary for the proper performance of a documented agency function. We have successfully completed our FY 2012 review. Thus, no further action is required at this time.

Please contact me with any questions. 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

MEMORANDUM

Date: November 15, 2012

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the *Federal Information Security Management Act of 2002* for Fiscal Year 2012 (A-14-12-12120)

The attached report summarizes our Fiscal Year (FY) 2012 evaluation of the Social Security Administration's (SSA) 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 each 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 2012 Inspector General FISMA reporting questions, is to be submitted through CyberScope pursuant to Department of Homeland Security Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

We determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements for FY 2012. However, weaknesses in some components of the program limited the program's overall effectiveness to adequately protect the Agency's information and information systems. As a result, we are reporting a FISMA significant deficiency in the Agency's information security program for FY 2012. 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

**THE SOCIAL SECURITY ADMINISTRATION'S
COMPLIANCE WITH THE *FEDERAL INFORMATION
SECURITY MANAGEMENT ACT OF 2002*
FOR FISCAL YEAR 2012**

November 2012

A-14-12-12120

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.

MEMORANDUM

Date: November 15, 2012

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the *Federal Information Security Management Act of 2002* for Fiscal Year 2012 (A-14-12-12120)

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Management Act of 2002* (FISMA) as defined by the Department of Homeland Security (DHS).

BACKGROUND

FISMA provides the framework for securing the Government's information and information systems. All agencies must implement the FISMA requirements and report annually to the Office of Management and Budget (OMB), 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.¹ Each agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.²

FISMA also requires that each agency's Inspector General (IG), or an independent external auditor, perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.³ Each evaluation shall

- test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and

¹ Pub. L. No. 107-347, Title III, Section 301 § 3544(b); 44 U.S.C. § 3544(b).

² Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A); 44 U.S.C. § 3544(a)(1)(A).

³ Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(1) and (b)(1); 44 U.S.C. §§ 3545(a)(1) and (b)(1).

- assess compliance with FISMA requirements, and related information security policies, procedures, standards, and guidelines.⁴

DHS is responsible for overseeing compliance with FISMA and developing analyses to assist in OMB's annual report to Congress on Federal agencies' compliance with FISMA.⁵ To fulfill its responsibilities, DHS provided annual FISMA reporting instructions for Federal agencies, including IGs. Specifically for IGs, DHS defined 11 FISMA security program components. For each component, IGs must respond to the following areas.

1. Has the Agency established an enterprise-wide program consistent with FISMA requirements, OMB policy, and applicable National Institute of Standards and Technology (NIST) guidance? If yes, besides the improvement opportunities that may have been identified by the IG, does the program include the attributes identified by DHS?
2. Provide any additional information on the effectiveness of the program.

SCOPE AND METHODOLOGY

We contracted with Grant Thornton, LLP, (GT) to audit SSA's Fiscal Year (FY) 2012 financial statements.⁶ Because of the extensive internal control system review completed as part of that work, some of our FISMA requirements were incorporated into GT's financial statement audit information technology (IT)-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, NIST guidance, the *Federal Information System Controls Audit Manual*, and other relevant security laws and regulations. We evaluated GT's work and performed additional FISMA testing for this review.

To assess whether SSA met FISMA requirements as defined by DHS, we used DHS guidance⁷ to test the compliance and effectiveness of agencies' security policies, procedures and practices. For the 11 FISMA security program component metrics and our responses to those metrics, see Appendix B, *Office of the Inspector General Response to FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*.

⁴ Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(2)(A) and (B); 44 U.S.C. §§ 3545(a)(2)(A) and (B).

⁵ OMB, 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, page 2.

⁶ Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009. The FY 2012 option was exercised in December 2011.

⁷ DHS, *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012.

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

RESULTS OF REVIEW

For FY 2012, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements.⁸ However, weaknesses in some of the program's components limited the overall program's effectiveness to adequately protect the Agency's information and information systems. Specifically, GT identified a material weakness over internal controls in its *Independent Auditor's Report*. We also identified additional weaknesses. Based on our evaluation of GT's work and our work, we believe these weaknesses constituted a significant deficiency under FISMA.

FINANCIAL STATEMENT AUDIT MATERIAL WEAKNESS

In FY 2012, GT identified deficiencies in information security controls that, when combined, it considered a material weakness. **A material weakness for financial statement purposes** 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 timely.⁹ As a result, for FY 2012, GT reported a material weakness in SSA's internal control over its financial statements.

GT stated that SSA had attempted to strengthen controls over its systems and address the outstanding significant deficiency in information security. However, GT's FY 2012 testing identified the following security weaknesses that, when aggregated, met the definition of a material weakness for financial statement purposes.

- [Lack of monitoring and policy implementation related to the configuration and information content of SSA's Intranet Webpages](#). The misconfiguration of some of SSA systems allowed GT to obtain security information and personally identifiable

⁸ Our conclusion was based on our assessment of SSA's compliance with DHS' *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012. As indicated in Appendix B, we determined that SSA established all 11 security program components, which were generally consistent with Federal guidance. The 11 components established by SSA included the vast majority of attributes identified by DHS. However, we also noted improvement opportunities for many attributes.

⁹ The definition of a material weakness for financial statement internal control is provided by the Statement on Auditing Standards Number 115, *Communicating Internal Control-Related Matters Identified in an Audit*.

information (PII)¹⁰ from SSA's Intranet. This issue increases the risk that SSA's sensitive information could be used inappropriately.

- **Lack of controls related to the identification and monitoring of high-risk programs operating on the Agency's mainframe.**¹¹ SSA did not conduct impact assessments to determine whether significant changes to its mainframe programs created any security implications. In addition, SSA management did not have a comprehensive process to periodically review privileged programs added to SSA's mainframe environment. Privileged programs are considered high-risk because they could bypass mainframe system security.
- **Insufficient vulnerability testing conducted by the Agency to identify critical weaknesses in its IT environment.** For the second year in a row, GT was able to gain access to restricted information and take control of SSA's Windows network during internal penetration testing.¹² GT reported that management's failure to conduct robust enterprise-focused penetration testing increases the risk that unauthorized access may occur and go undetected, allowing privileged information or critical infrastructure to be compromised.
- **Lack of a comprehensive profile and access recertification program.** GT found that SSA developed identity and access management policies and procedures to periodically reassess the content of security access profiles.¹³ However, the Agency had not consistently implemented these policies and procedures. Further, GT's testing identified personnel with inappropriate access.
- **Lack of appropriate controls to prevent unauthorized access to the Agency's production environment.** Agency management stated that a control was in place to allow programmers highly monitored and time-limited access to production data. However, GT identified software programmers with access to SSA's production data that bypassed this control. SSA management indicated this issue resulted from

¹⁰ OMB, M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006, page 1, defines PII as any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information 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.

¹¹ International Business Machines Corp. defines a mainframe as computers that can support thousands of applications and input/output devices to simultaneously serve thousands of users. A mainframe is the central data repository, or hub, in a corporation's data processing center, linked to users through less powerful devices such as workstations or terminals.

¹² GT used a different method to take control of SSA's Windows network this year.

¹³ 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 a specific position needs.

human error, and that no current control would have identified this error in a timely manner. In addition, GT identified instances where this control was used, but access was not timely approved and reviewed. Despite these weaknesses, GT did not find any unauthorized changes to the Agency's data.

WEAKNESSES IN SOME COMPENSATING CONTROLS

GT discussed the security weaknesses it identified with SSA management and staff. Agency management stated that compensating controls existed to mitigate the risks created by the security weaknesses. However, GT's FY 2012 financial statement audit testing and our audits identified weaknesses in some of the compensating controls identified by SSA. This included control deficiencies in the Agency's change control process and physical and logical access controls. For example, GT noted weaknesses over the approval and documentation for changes to SSA software applications. Further, we found that a contractor employee maintained physical access to SSA facilities for approximately 1 year after the contractor employee was deemed unsuitable for employment.¹⁴ In addition, we found that a disability determination services' employee's system user identification was used after the employee was terminated.¹⁵

ADDITIONAL SECURITY WEAKNESSES

In addition to the security weaknesses identified above, our FY 2012 FISMA testing identified some security weaknesses related to key components of SSA's information security program. These key components include Continuous Monitoring, Configuration Management, Identity and Access Management, Risk Management, and Contractor Systems Oversight. In prior years, we have also identified weaknesses in these areas. We highlight some key weaknesses below.

- **Continuous Monitoring:**¹⁶ The Agency had not fully implemented its continuous monitoring strategy. For example, SSA had not implemented compliance monitoring tools for all of its platforms.¹⁷ Further, SSA needed to assess and validate the technical capacity of each continuous monitoring tool to meet NIST requirements. Finally, SSA's continuous monitoring activities did not provide the near real-time information required for Agency officials to proactively manage the Agency's information security program in accordance with OMB and NIST requirements.

¹⁴ The contractor employee was immediately removed from the contract after the appropriate SSA personnel were notified.

¹⁵ Management confirmed that no transactions were executed with the terminated employee's user identification after termination.

¹⁶ Continuous Monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

¹⁷ A platform is a hardware and/or software architecture that serves as a foundation or base. An operating system, like Windows, is an example of a platform.

- **Configuration Management:**¹⁸ SSA used risk models for its platforms to prescribe security settings and manage risk. However, SSA had not documented risk models for all of its platforms. Further, the Agency did not perform vulnerability scans of all platforms to determine whether prescribed security settings were implemented. Moreover, the vulnerability scans and penetration testing performed by GT identified a number of security weaknesses.
- **Identity and Access Management:**¹⁹ SSA scanned its network to identify connected hardware, but as of the date of this review, it had been unable to categorize all types of hardware and their associated operating systems.
- **Risk Management:**²⁰ SSA had weaknesses in its security governance structure. The Agency's central technical security component did not have control over regional office Intranet Websites. In addition, SSA lacked a centralized process to authorize hardware devices before they were connected to the Agency's network.
- **Contractor Systems Oversight:**²¹ SSA did not maintain a complete inventory of all contractor systems and services and did not ensure all contractor systems and services met Federal security requirements. Specifically, we identified seven systems and services that met the FISMA criteria for contractor systems but either

¹⁸ From a security point of view, Configuration Management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications.

¹⁹ Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files. The identification of devices with Internet Protocol addresses attached to an agency's network is included under the Identity and Access Management section of DHS' *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012.

²⁰ "Risk Management is 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." NIST Special Publication 800-53, Rev. 3, page B-11.

²¹ Agencies are responsible for ensuring that appropriate security controls are in place over contractor systems used or operated by contractors or other entities (such as other Federal or state agencies) on behalf of an agency. We used OMB M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Frequently Asked Questions, September 27, 2012, pages 15 to 16, to determine the purview of the Agency's FISMA responsibilities for contractor systems. SSA disagreed with our interpretation. However, this OMB guidance explicitly provides that "Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which process, store, or transmit Federal information- or which operate, use, or have access to Federal information systems (whether automated or manual) -on behalf of a Federal agency." OMB, M-12-20 at page 16.

were not included in the Agency's systems inventory or were not identified as a contractor system or service, as required by FISMA guidance. Further, some of SSA's contracts did not include Federal security requirements, as required by FISMA guidance.

FISMA SIGNIFICANT DEFICIENCY

OMB defines a FISMA 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.”²²

SSA administers two of the nation's largest entitlement programs, the Old-Age, Survivors, and Disability insurance program and the Supplemental Security Income program. These programs touch the lives of virtually every American. It is imperative that SSA protect these programs by ensuring the safety and security of its information systems and the data contained in them.

Based on our evaluation of the work performed by GT and the results of our additional FISMA work, we concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a significant deficiency under FISMA. These weaknesses could result in losses of confidentiality, integrity, and availability of SSA information systems and data.²³ Given the complex systems and magnitude of sensitive information housed on SSA's systems, any loss of confidentiality, integrity, or availability of Agency systems or data could have a significant impact on the public and the nation's economy. For example, during its internal penetration testing, GT was able to take control of SSA's Windows network and obtain many records containing PII. In addition, GT noted concerns related to the identification and monitoring of high risk programs operating on the mainframe. Without performing specific assessments of the impact of program changes to the system security framework, there is an increased risk that the security posture and controls may be bypassed or compromised. Finally, GT identified programmers with access to production data that bypassed SSA's process to monitor and limit such access. Specifically, GT identified programmers with unmonitored access to production data for a benefit application. This issue increases

²² OMB, M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, Frequently Asked Questions, September 27, 2012, page 26.

²³ **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. **Integrity** means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. **Availability** means ensuring timely and reliable access to and use of information. Pub. L. No. 107-347, Title III, Section 301 § 3542(b)(1)(A) to (C), 44 U.S.C. § 3542(b)(1)(A) to (C).

the risk that programmers could make unauthorized changes to the production environment without detection.

The security deficiencies identified above, when aggregated, created a weakness in SSA's overall information systems security program that, in our opinion, significantly compromised the security of its information and information systems. We also believe that the risk was great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.²⁴

UNDERLYING CAUSES FOR SSA'S FINANCIAL STATEMENT AUDIT MATERIAL WEAKNESS AND FISMA SIGNIFICANT DEFICIENCY

Based on our testing and evaluation of GT's work, we believe the following items caused the Agency's material weakness and FISMA significant deficiency.

1. SSA had not fully implemented a comprehensive and robust continuous monitoring program based on a sound configuration management program. Without a robust continuous monitoring program that includes integrated and operating continuous monitoring tools and the capacity to report SSA's security state to appropriate Agency officials, the Agency had a limited ability to make timely risk management decisions.
2. SSA had a decentralized governance structure for IT security. This resulted in a system misconfiguration that enabled GT, without detection, to obtain PII and take control of SSA's Windows network.
3. SSA needed to strategically allocate sufficient resources to resolve or prevent high-risk security weaknesses more timely. This includes the use of more effective security testing methods, such as broad penetration testing techniques.

AGENCY EFFORTS TO RESOLVE SECURITY WEAKNESSES

It should be noted that SSA took action to address some of its security weaknesses identified by GT and us:

[Lack of monitoring and policy implementation related to the configuration and information content of SSA's Intranet Webpages.](#) SSA stated it was conducting a Web vulnerability assessment. In addition, the Agency stated it had purchased and was deploying a data loss protection tool.

[Lack of controls related to the identification and monitoring of high-risk programs operating on the Agency's mainframe.](#) The Agency removed one high-risk privileged

²⁴ Significant deficiencies identified under FISMA must be reported as material weaknesses in the annual *Federal Managers' Financial Integrity Act of 1982* report. OMB Circular A-123 Revised, *Management's Responsibility for Internal Control*, Section IV B, December 21, 2004.

program identified by GT. Furthermore, SSA stated it was expanding its review process to include all mainframe privileged programs.

Insufficient vulnerability testing conducted by the Agency to identify critical weaknesses in its IT environment. SSA documentation indicated that over the past 10 years, the Agency has performed some penetration testing. Between 2009 and 2011, SSA used some of the funding traditionally used for penetration testing for other information security purposes. However, SSA stated that in 2012, it began performing penetration testing with an open and dynamic scope. The Agency hired three contractor employees in September 2012 to perform targeted internal penetration testing to identify security weaknesses of SSA's networks.

Lack of a comprehensive profile and access recertification program. In FY 2011, SSA issued two policies governing security profiles.²⁵ In addition, the Agency assembled a workgroup to address its access control weaknesses. The workgroup tested a commercial tool to manage the profile review process for SSA employee and contractor access. The Agency began using the tool in FY 2012. SSA planned to remediate some access control issues by fully implementing its profile and access recertification program in early FY 2013.

Lack of appropriate controls to prevent unauthorized access to the Agency's production environment. SSA management stated that the Agency removed the access of the programmers identified in GT's testing. Moreover, the Agency stated its triennial access recertification will identify these issues in the future, and SSA was exploring options to alert the Agency if programmers gain access to the production environment.

Continuous monitoring strategy not fully implemented. SSA developed a continuous monitoring strategy, but the strategy had not been fully implemented. SSA discussed its preliminary plan to implement its continuous monitoring strategy with us. To build upon its continuous monitoring strategy, SSA has been evaluating the ability of its continuous monitoring tools to ensure compliance with Federal requirements and Agency policies and procedures. Further, SSA management stated that after the continuous monitoring tool evaluations are completed, it will have a better idea of the timeframe needed to fully implement its continuous monitoring strategy. The Agency plans to complete the continuous monitoring tool evaluations by the end of calendar year 2012. Finally, SSA is evaluating which security deficiencies identified by GT could be resolved by fully implementing its continuous monitoring strategy.

²⁵ SSA, *Security Profile Administration Processes Final Mainframe Administration Standards*, May 10, 2011, and SSA, *Security Profile Administration Processes Profile Naming Conventions*, October 28, 2010.

CONCLUSION AND RECOMMENDATIONS

For FY 2012, we determined that SSA's overall information security program and practices were generally consistent with FISMA requirements. However, weaknesses in some components of the program limited the overall program's effectiveness to adequately protect the Agency's information and information systems. We noted that GT reported a material weakness over SSA's internal controls for the Agency's financial statement audit. After considering this material weakness, its underlying causes, and the results of our FISMA-related work, we concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a significant deficiency under FISMA.

SSA needed to effectively protect its mission-critical assets. Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. Some weaknesses identified in this report could cause the Agency's systems and data to lose confidentiality, integrity, and availability to some degree. Given the complex systems and magnitude of sensitive information housed on SSA's systems, any loss of the confidentiality, integrity, or availability of Agency systems or data could have a significant impact on the public.

To improve the effectiveness of SSA's overall information security program and to address the material weakness, GT recommended that SSA management consider implementing:

- Monitoring controls designed to identify configurations in the SSA network and systems environment that do not comply with the SSA system configuration policy. In addition, management should consider implementing controls to identify and track content on SSA's Intranet Webpages that may pose a risk to the security of SSA systems or the confidentiality of SSA data.
- A comprehensive program to identify and monitor high-risk programs operating on the mainframe. Consider including the identification of programs that may pose security risks to the SSA mainframe before they are loaded onto the production environment.
- Comprehensive enterprise-wide security vulnerability testing, including simulated penetration attacks, to identify critical weaknesses in the IT environment that may not be identified by the current control processes.
- A comprehensive profile and access recertification program.
- Additional controls to prevent unauthorized programmer access to the production environment.

We reiterate GT's recommendations and believe these recommendations address the financial statement audit material weakness and FISMA significant deficiency. In addition, our prior FISMA reports identified issues related to SSA's (1) continuous monitoring, (2) configuration management, (3) identity and access management, (4) risk

management, and (5) contractor systems oversight. We affirm our prior recommendations in these areas and encourage the Agency to continue implementing them.

A handwritten signature in black ink, appearing to read "Pat P. O'Carroll, Jr.", with a stylized flourish at the end.

Patrick P. O'Carroll, Jr.

Appendices

APPENDIX A – Acronyms

APPENDIX B – Office of the Inspector General Response to *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*

APPENDIX C – Scope and Methodology

APPENDIX D – The Social Security Administration's Major Systems

APPENDIX E – OIG Contacts and Staff Acknowledgments

Acronyms

DHS	Department of Homeland Security
FISMA	<i>Federal Information Security Management Act of 2002</i>
FY	Fiscal Year
GT	Grant Thornton LLP
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
SSA	Social Security Administration
U.S.C.	United States Code

Office of the Inspector General Response to *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*¹

Section 1: CONTINUOUS MONITORING MANAGEMENT

- 1.1. Has the Organization 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?**

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

- 1.1.1. Documented policies and procedures for continuous monitoring.**

Yes

- 1.1.2. Documented strategy and plans for continuous monitoring.**

Yes

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

Yes

Comments: To date, SSA had not fully implemented its continuous monitoring program. For example, the Agency had not developed risk models for some of the hardware and software connected to its network. Therefore, the Agency did not continually monitor these operating system platforms and applications.

- 1.1.4. 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.**

¹ Department of Homeland Security (DHS), *FY 2012 Inspector General Federal Information Security Management Act Reporting Metrics*, March 6, 2012. We extracted the DHS metrics as they were written in the document without editing, except for the citations to Federal guidance at the end of some metrics that we omitted for consistency.

Yes

Comments: SSA's current continuous monitoring could not provide a comprehensive view and near real-time information of the enterprise.

- 1.2. Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above.

Comments: SSA did have a continuous monitoring strategy, but it had not been fully implemented. For example, SSA had identified, evaluated, and implemented, some continuous monitoring tools for its operating environment. However, the Agency needed additional time to ensure the continuous monitoring tools were fully operable within its information system environment. Consequently, SSA's continuous monitoring program could not provide a comprehensive view and near real-time information of the enterprise.

Weaknesses identified in this area contributed to a financial statement audit material weakness identified by Grant Thornton, LLP (GT). Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 2: CONFIGURATION MANAGEMENT

- 2.1. Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

- 2.1.1. Documented policies and procedures for configuration management.

Yes

- 2.1.2. Standard baseline configurations defined.

Yes

Comments: The Agency had established baseline configurations for many, but not all, computer platforms.

- 2.1.3. Assessing for compliance with baseline configurations.

Yes

Comments: We identified security weaknesses in the configuration settings of some SSA computer platforms. Internal penetration

testers were able to obtain security information and personally identifiable information because some of SSA's systems were misconfigured. SSA had taken corrective action to address these issues.

2.1.4. Process for timely, as specified in Organization policy or standards, remediation of scan result deviations.

Yes

2.1.5. For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented.

Yes

2.1.6. Documented proposed or actual changes to hardware and software configurations.

Yes

Comments: SSA monitored the hardware devices connected to its network to determine whether they complied with approved risk models and configuration settings. However, the Agency did not conduct impact assessments to determine the security implications for system changes. In addition, management did not have a formally documented process to periodically review the privileged programs added to the Agency's mainframe environment to ensure that all privileged programs are approved, cannot be improperly modified, and are safe. We also identified discrepancies in the approval and documentation of changes to SSA applications.

2.1.7. Process for timely and secure installation of software patches.

Yes

2.1.8. Software assessing (scanning) capabilities are fully implemented.

No

Comments: The Agency had implemented scanning procedures for some, but not all, platforms. SSA did not have a formal process in place for managing or obtaining a comprehensive list of approved software for all devices. However, the Agency had made efforts to develop this process.

2.1.9. Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards.

Yes

Comments: Annual vulnerability scans and penetration testing have consistently identified security weaknesses. However, some security weaknesses were fully or partially remediated during the

audit period. Since the Agency does not have risk models for all computer platforms, some configuration-related vulnerabilities went unidentified.

2.1.10. Patch management process is fully developed, as specified in Organization policy or standards.

Yes

2.2. Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 3: IDENTITY AND ACCESS MANAGEMENT

3.1. Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices?

Yes

If yes, besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:

3.1.1. Documented policies and procedures for account and identity management.

Yes

3.1.2. Identifies all users, including federal employees, contractors, and others who access Organization systems.

Yes

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

Yes

Comments: We identified programmers with access to production data that bypassed SSA's process to monitor and limit such access.

3.1.4. If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate.

Yes

3.1.5. Organization has adequately planned for implementation of PIV for logical access in accordance with government policies.

Yes

- 3.1.6. Ensures that the users are granted access based on needs and separation of duties principles.**

Yes

Comments: Although SSA had an extensive access control program, internal penetration testers were able to take control of SSA's Windows network. Testing also identified personnel with inappropriate access and programmers with access to production data that bypassed SSA's process to monitor and limit such access. The Agency had not consistently implemented policies and procedures to periodically reassess the content of security access profiles. SSA was working to improve its profile and access recertification program and planned for a full implementation in Fiscal Year (FY) 2013.

- 3.1.7. Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)**

Yes

Comments: Although SSA scanned its network to identify hardware devices connected to it, the Agency had been unable to categorize all hardware devices and their associated operating systems connected to its network. Further, SSA did not have an automated capability to determine whether hardware devices connected to its network were authorized.

- 3.1.8. Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)**

Yes

- 3.1.9. Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

Comments: Although SSA had policies and procedures to terminate access when it is no longer needed, we identified instances where physical and logical access was not removed timely.

3.1.10. Identifies and controls use of shared accounts.

Yes

3.2. Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 4: INCIDENT RESPONSE AND REPORTING

4.1. Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

4.1.1. Documented policies and procedures for detecting, responding to and reporting incidents.

Yes

4.1.2. Comprehensive analysis, validation and documentation of incidents.

Yes

4.1.3. When applicable, reports to US-CERT within established timeframes.

Yes

4.1.4. When applicable, reports to law enforcement within established timeframes.

Yes

Comments: SSA reported incidents to OIG in a timely manner. The Agency did not have an established timeframe for reporting incidents to external law enforcement or the Federal Protective Services. SSA identified incidents reported to external law enforcement or the Federal Protective Services; however, the Agency did not provide police reports for sampled incidents.

4.1.5. Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage.

Yes

4.1.6. Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.

Yes

4.1.7. Is capable of correlating incidents.

Yes

4.1.8. There is sufficient incident monitoring and detection coverage in accordance with government policies.

Yes

4.2. Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.

N/A

Section 5: RISK MANAGEMENT

5.1. Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

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

Yes

5.1.2. 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

Comments: SSA had a decentralized governance structure for IT security. This resulted in a system misconfiguration going undetected, enabling GT to obtain security and personally identifiable information. In addition, SSA lacked a centralized process to authorize hardware devices before they were connected to the Agency's network.

5.1.3. 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

5.1.4. 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

5.1.5. Categorizes information systems in accordance with government policies.

Yes

5.1.6. Selects an appropriately tailored set of baseline security controls.

Yes

5.1.7. 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

5.1.8. 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

Comments: Financial statement audit testing found that SSA's vulnerability testing was insufficient.

5.1.9. 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

5.1.10. 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

Comments: SSA performed security authorizations and annual security testing of selected controls. However, SSA's continuous monitoring program was not fully implemented. See comment for Metric 1.2.

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

Yes

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

Yes

5.1.13. 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

5.1.14. Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies.

Yes

5.1.15. Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

Yes

5.2. Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

Comments: Weaknesses identified in this area contributed to a financial statement audit material weakness identified by GT. Based on our work and evaluation of GT's work, we concluded that SSA had a FISMA significant deficiency.

Section 6: SECURITY TRAINING

6.1. Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

6.1.1. Documented policies and procedures for security awareness training.

Yes

6.1.2. Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

6.1.3. Security training content based on the organization and roles, as specified in Organization policy or standards.

Yes

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

Yes

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

Yes

6.1.6. Training material for security awareness training contains appropriate content for the Organization.

Yes

6.2. Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.

N/A

Section 7: PLAN OF ACTION & MILESTONES (POA&M)

7.1. Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation.

Yes

Comments: SSA's policy needed to be updated to reflect the current tools used to monitor and track security weaknesses.

7.1.2. Tracks, prioritizes and remediates weaknesses.

Yes

Comments: We found some IT security risks that were tracked, but not prioritized.

7.1.3. Ensures remediation plans are effective for correcting weaknesses.

Yes

7.1.4. Establishes and adheres to milestone remediation dates.

Yes

Comments: We noted several POA&Ms that did not include a scheduled completion date.

7.1.5. Ensures resources are provided for correcting weaknesses.

Yes

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control).

Yes

7.1.7. Costs associated with remediating weaknesses are identified.

Yes

7.1.8. 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

7.2. Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.

N/A

Section 8: REMOTE ACCESS MANAGEMENT

8.1. Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

8.1.1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.

Yes

8.1.2. Protects against unauthorized connections or subversion of authorized connections.

Yes

8.1.3. Users are uniquely identified and authenticated for all access.

Yes

8.1.4. Telecommuting policy is fully developed.

Yes

Comments: SSA's revised telework policy was in draft form, pending the resolution of administrative matters.

8.1.5. If applicable, multi-factor authentication is required for remote access.

Yes

8.1.6. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

8.1.7. Defines and implements encryption requirements for information transmitted across public networks.

Yes

8.1.8. 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

Comments: SSA exceeded best practice since its sessions time-out after 15 minutes of inactivity.

8.1.9. Lost or stolen devices are disabled and appropriately reported.

Yes

8.1.10. Remote access rules of behavior are adequate in accordance with government policies.

Yes

8.1.11. Remote access user agreements are adequate in accordance with government policies.

Yes

8.2. Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.

N/A

Section 9: CONTINGENCY PLANNING

9.1. Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

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

Yes

9.1.2. The Organization has performed an overall Business Impact Analysis (BIA).

Yes

9.1.3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.

Yes

9.1.4. Testing of system specific contingency plans.

Yes

Comments: The Agency did not conduct contingency plan testing for 2 of the 21 major systems/applications. For one of the applications, the application owners were not aware of the annual testing requirement. For the other application, the application owners were working with the appropriate subject matter experts to integrate their application into SSA's disaster recovery exercise.

9.1.5. The documented business continuity and disaster recovery plans are in place and can be implemented when necessary.

Yes

9.1.6. Development and fully implementable of test, training, and exercise (TT&E) programs.

Yes

9.1.7. Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans.

Yes

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises.

Yes

9.1.9. Systems that have alternate processing sites.

Yes

9.1.10. Alternate processing sites are subject to the same risks as primary sites.

Yes

9.1.11. Backups of information that are performed in a timely manner.

Yes

9.1.12. Contingency planning that consider supply chain threats.

Yes

Comments: SSA's two data centers will back up each other. SSA considered supply chain threats for one data center, but not the other.

9.2. Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.

N/A

Section 10: CONTRACTOR SYSTEMS

10.1. Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:

10.1.1. Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.

Yes

10.1.2. The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines.

Yes

Comments: For 12 of 17 contractor systems identified by our testing, SSA either performed a security authorization or obtained documentation of the systems' compliance with Federal security guidelines. Three of the contractor systems were operated or owned by other Federal or State agencies. One was operated by a contractor whose services were used by many Federal agencies. SSA believed it was not responsible for performing a security authorization of this contractor system. The remaining contractor system was a Website, located in a public cloud, but did not have the proper security authorization. However, the Website contained non-sensitive, public information, and a link that redirected users to SSA's secure Website to report fraud allegations.

10.1.3. A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud.

No

Comments: We found seven contractor systems that SSA had not identified on its inventory list.

10.1.4. The inventory identifies interfaces between these systems and Organization-operated systems.

Yes

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

Yes

10.1.6. The inventory of contractor systems is updated at least annually.

Yes

10.1.7. Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

Yes

Comments: See comments for Metric 10.1.2.

10.2. Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.

Comments: We found some IT-related contracts did not contain the proper FISMA security clause requirements.

Section 11: SECURITY CAPITAL PLANNING

11.1. Has the Organization established a security capital planning and investment program for information security?

Yes

If yes, besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

11.1.1. Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.

Yes

11.1.2. Includes information security requirements as part of the capital planning and investment process.

Yes

11.1.3. Establishes a discrete line item for information security in organizational programming and documentation.

Yes

11.1.4. Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.

Yes

Comments: We identified inconsistencies in the supporting documents for some line items in Exhibit 53B. For example, some Exhibit 53B numbers were based on budget estimates rather than budget decisions.

11.1.5. Ensures that information security resources are available for expenditure as planned.

Yes

11.2. Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

N/A

Scope and Methodology

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Inspector General 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. We contracted with Grant Thornton LLP (GT) to audit the Social Security Administration's (SSA) Fiscal Year (FY) 2012 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 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; Department of Homeland Security (DHS) Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*; National Institute of Standards and Technology guidance; the *Federal Information System Controls Audit Manual*; and other relevant security laws and regulations as a framework to complete the Inspector General-required review of SSA's information security program and practices and its information systems.

The results of our FISMA review are based on our evaluation of GT's FY 2012 financial statement audit and agreed-upon procedures work papers as well as various audits by our office. We also reviewed SSA's draft 2012 FISMA *Chief Information Officer Section Report*.

Our evaluation followed the DHS FY 2012 FISMA guidance¹ and focused on Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plan 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 April to October 2012. We considered the results of our other audits performed in FY 2012. 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 DHS Federal Information Security Memorandum 12-02, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, February 15, 2012.

The Social Security Administration’s Major Systems

	System	Acronym
	General Support Systems¹	
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 and System	EWANS
6	FALCON Data Entry System	FALCON
7	Human Resources Management Information System	HRMIS
8	Integrated Client Database System	ICDB
9	Integrated Disability Management System	IDMS
10	Quality System	QA
11	Security Management Access Control System	SMACS
12	Social Security Online Accounting & Reporting System	SSOARS
13	Social Security Unified Measurement System	SUMS
	Major Applications²	
1	Electronic Disability System	eDib

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
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR
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, Audit Manager

Acknowledgments

In addition to those named above:

Michael Zimmerman, Auditor- in-Charge

Tina Nevels, Auditor-in-Charge

Asad Isfahani, Auditor

For additional copies of this report, please visit our Website at <http://oig.ssa.gov/> or contact the Office of the Inspector General's Public Affairs Staff at (410) 965-4518. Refer to Common Identification Number A-14-12-12120.

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.