



SOCIAL SECURITY
The Commissioner

November 26, 2013

The Honorable Sylvia Mathews Burwell
Director, Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Ms. Mathews Burwell:

We are pleased to submit our fiscal year 2013 Information Technology Security Program Review Report, as required by the Federal Information Security Management Act (FISMA). Our submission includes the reports of our Chief Information Officer, 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.

Our financial statement auditors found that we made significant progress in strengthening controls over our information systems to address the material weakness the auditors found last year. In this year's financial statement audit, the auditors reduced the severity of their finding to a significant deficiency. However, our OIG cited the auditors' finding as a significant deficiency under FISMA. FISMA requires that we report the significant deficiency as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA) and as a lack of substantial compliance with the Federal Financial Management Improvement Act (FFMIA) if related to financial management systems.

We do not believe that the significant deficiency rises to the level of a material weakness under FMFIA. Further, we believe that we are substantially compliant with FFMIA, as this finding does not prevent us from providing reliable and timely financial information. We also believe that we are substantially compliant with the requirements of FISMA to provide adequate and effective information security policies, procedures, and practices. As we do with all auditor findings, we will continue to aggressively pursue a risk-based corrective action plan to address the remaining deficiency and build on our progress to date.

If you have any questions about this information, please have your staff contact Bill Zielinski, our Chief Information Officer, at (410) 965-4380, or by email at Bill.Zielinski@ssa.gov.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure

FY 2013 FISMA

Senior Agency Official for Privacy Report

Description of the Agency's Privacy Training for Employees and Contractors

The Social Security Administration (SSA) recognizes the importance of providing privacy training to all of our employees and contractors. Our regulations (20 C.F.R. § 401.30(e)) provide that the Senior Agency Official for Privacy (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 Personally Identifiable Information (PII) and adherence to the Privacy Act and other provisions. The agency's Program Operations Manual System (POMS) is a primary source of information used by our employees and contractors. Specifically, Chapter GN 033 of our POMS contains instructions that apply to the disclosure of personal information in our records.

In 2013, we continued to devote time and resources to hosting privacy education and awareness activities, including several Videos on Demand (VOD) via our Office of Learning. We provide specialized training on the Privacy Act, and related privacy regulations, policies, and procedures. For example, employees have access to four specific VODs on protecting and safeguarding PII. In FY 2013, we also continued our practice of training systems development staff on the importance of privacy and privacy risk assessment via the System Development Life Cycle (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, the Office of Management and Budget (OMB), and the CIO Council to ensure that their expertise remains current.

Chief Information Officer

Section Report

2013

Annual FISMA
Report

Social Security Administration

Section 1: Systems Inventory

- 1.1 For each of the FIPS 199 systems' categorized impact levels (H = High, M = Moderate, L = Low) in this question, what is the total number of information systems by organization (i.e. Bureau or Sub-Department Operating Element)? Answer in Table 1 below. (Organizations with fewer than 5000 users may report as one unit.)

		1.1.1 Organization Operated Systems	1.1.2 Contractor Operated Systems	1.1.3 Systems (from 1.1.1 and 1.1.2) with Security ATO
SSA	High	0	0	0
	Moderate	16	0	16
	Low	5	0	5
	Not Categorized	0	0	0
	Sub-Total	21	0	21
The SSA inventory process accounts for the contractor/cloud systems by incorporating them into larger system authorization boundaries. These contractor/cloud components are documented accordingly in the applicable system security plans.				
Agency Totals	High	0	0	0
	Moderate	16	0	16
	Low	5	0	5
	Not Categorized	0	0	0
	Total	21	0	21

Section 2: Asset Management

- 2.1** What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?
278266
- 2.2** What percentage of assets in 2.1 have an automated capability (scans/device discovery processes) to provide enterprise-level visibility into asset inventory information for all hardware assets?
100%
- 2.2.1** How often are these automated capabilities (scans/device discovery processes) conducted on all assets connected to the organization's full network(s)? Report the lowest frequency of automated device discovery on any applicable network of the organization. In the comments, you may include an average time weighted by assets per discovery frequency, if desired.
14.0
- 2.3** For how many assets in 2.1 does the organization have an automated capability to determine both whether the asset is authorized and to whom management has been assigned?
262689
- 2.4** Can the organization track the installed operating system's vendor, product, version, and patch-level combination(s) in use on the assets in 2.1?
Yes
- 2.4.1** If yes, report the number of patch-level combinations. We assume one operating system per device. In the comments, report the number of devices that can boot with multiple operating systems. Note that virtual machines should be counted as assets.
24
- Comments:** SSA has 481 devices that can boot with multiple operating systems.
- 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 2.1?
Yes
- 2.5.1** If yes, report the number of general-purpose applications.
38
- 2.6** For what percentage of applicable assets in 2.1 has the organization implemented an automated capability to detect and block unauthorized software from executing, or for what percentage does no such software exist for the device type? This may include software whitelisting tools that identify executable software by a digital fingerprint and selectively block these. It might also include sandboxing of mobile code to determine before execution whether to allow it to run, where static files do not allow whitelisting. In general, any method included should be able to block zero-day and APT threats.
0%

Section 2: Asset Management

Comments: SSA has not implemented an automated capability to detect and block unauthorized software.

Section 3: Configuration Management

3.1 For each operating system vendor, product, and patch-level combination referenced in 2.4, report the following:

Comments: "OTHER" applies to: 91,229 Voice Over IP Devices | 15,562 Printers/Multi-Function Devices | 8,690 Routers & Switches | 536 Wireless Access Points.

Vendor/Operating System/Version	3.1.1 Has an adequately secure configuration baseline been defined?	3.1.2 How many hardware assets (which are covered by this baseline, if it exists) have this software?	3.1.3 What percentage of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1 have an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level?	3.1.4 What is the frequency of deviation identification (answer in days, per General Instructions)?
Apple Mac OS	No	15	0 %	0.000
Blackberry OS 10.0	Yes	4192	100 %	1.000
HP-UX 11 family	Yes	52	100 %	14.000
IBM AIX 5	Yes	2	100 %	14.000
IBM AIX 6.1	Yes	9	100 %	14.000
IBM OS_400	Yes	53	100 %	53.000
IBM z/OS	Yes	62	100 %	62.000
Microsoft Windows Server 2003	Yes	781	100 %	6.000
Microsoft Windows 2003 Server Standard Edition R2	Yes	1125	100 %	6.000
Microsoft Windows 7 x64 (64-bit)	Yes	144809	100 %	6.000
Microsoft Windows Server 2008 Service Pack 1	Yes	170	100 %	6.000
Microsoft Windows Server 2008 Service Pack 2	Yes	365	100 %	6.000
Microsoft Windows Server 2008 R2	Yes	255	100 %	6.000
Microsoft Windows Server 2008 R2 Service Pack 1	Yes	7011	100 %	6.000
Microsoft Windows Server 2012	Yes	646	100 %	6.000
Microsoft Windows Vista x64 (64-bit)	Yes	1348	100 %	6.000
OTHER	Yes	91229	100 %	1.000

Section 3: Configuration Management

Vendor/Operating System/Version	3.1.1 Has an adequately secure configuration baseline been defined?	3.1.2 How many hardware assets (which are covered by this baseline, if it exists) have this software?	3.1.3 What percentage of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1 have an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and to provide visibility at the organization's enterprise level?	3.1.4 What is the frequency of deviation identification (answer in days, per General Instructions)?
OTHER	No	15562	0 %	0.000
OTHER	Yes	8690	100 %	1.000
OTHER	Yes	536	100 %	1.000
Red Hat Linux 6.0	Yes	17	100 %	14.000
Sun SunOS (formerly Solaris)	Yes	856	100 %	14.000
VMWare ESXi 4.0	Yes	3	0 %	0.000
VMWare ESXi 5.0	Yes	478	0 %	0.000

- 3.2 What percentage of network boundary devices is assessed by an automated capability to ensure that they are adequately configured as intended, such as to adequately protect security?
100%

Section 4: Vulnerability and Weakness Management

- 4.1 What percentage of network boundary devices is assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities?
100%
- 4.2 What percentage of hardware assets identified in section 2.1 are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level?
94%
- 4.2.1 What percentage of hardware assets identified in 2.1 that were evaluated using tools to assess the security of the systems and that generated output are compliant with each of the following?
- 4.2.1.1 Common Vulnerabilities and Exposures (CVE)
56%
- 4.2.1.2 Common Vulnerability Scoring System (CVSS)
56%

Section 4: Vulnerability and Weakness Management

4.2.1.3 Open Vulnerability and Assessment Language (OVAL)

56%

4.3 For what percentage of information systems does the organization do the following?

Impact Level	For systems in development and/or maintenance:		For systems in production:	
	Use methods described in FY13 CIO FISMA Metrics document Table 9, to identify and fix instances of common weaknesses, prior to placing that version of the code into production.	Can the organization 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 the organization find SCAP compliant tools and good SCAP content?
High	0%	Yes	0%	Yes
Moderate	100%	Yes	0%	Yes
Low	100%	Yes	0%	Yes

Section 5: Identity and Access Management

5.1 How many people have unprivileged network accounts? (Exclude privileged network accounts and non-user accounts.)

73790

5.2 What percentage of people with an unprivileged network account can log onto the network in each of the following ways?

5.2.1 Allowed to log on with user ID and password.

17%

Comments: This number solely consists of non-Federal, State employees awaiting SSA issued HSPD-12 credentials.

5.2.2 Allowed, but not required, to log on with a non-PIV form of two-factor authentication.

0%

Comments: SSA does not employ non-PIV two factor authentication for Windows.

5.2.3 Allowed, but not required, to log on with a two-factor PIV card.

0%

Comments: SSA policy requires all users with PIV cards to use them for network log on.

5.2.4 Required to log on with a non-PIV form of two-factor authentication.

0%

Section 5: Identity and Access Management

Comments: SSA does not employ non-PIV two factor authentication.

5.2.5 Required to log on with a two-factor PIV card.

83%

5.2.6 Required to conduct PIV authentication at the user-account level.

83%

Comments: All PIV user-account level authentication occurs at network login.

5.3 How many people have privileged network accounts? (Exclude unprivileged network accounts and non-user accounts.)

8743

5.4 What percentage of people with a privileged network account can log onto the network in each of the following ways?

5.4.1 Allowed to log on with user ID and password.

1%

Comments: This number accounts for SSA's Active Directory Domain Administrators.

5.4.2 Allowed, but not required, to log on with a non-PIV form of two-factor authentication.

0%

Comments: SSA does not employ non-PIV two factor authentication.

5.4.3 Allowed, but not required, to log on with a two-factor PIV card.

1%

Comments: This number accounts for SSA's Active Directory Domain Administrators.

5.4.4 Required to log on with a non-PIV form of two-factor authentication.

0%

Comments: SSA does not employ non-PIV two factor authentication.

5.4.5 Required to log on with a two-factor PIV card.

99%

5.4.6 Required to conduct PIV authentication at the user-account level.

99%

Comments: All PIV user-account level authentication occurs at network login.

5.5 What is the estimated number of organization internal systems?

Section 5: Identity and Access Management

21

5.6 What percentage of the organizations internal systems are configured for authentication in each of the following ways?

5.6.1 Allows user ID and password.

100%

Comments: Users are required via policy to access systems running on our network with PIV. We are working on the technical enforcement of the policy in FY14.

5.6.2 Allows, but does not enforce, non-PIV, two-factor authentication for users.

0%

5.6.3 Allows, but does not enforce, two-factor PIV card authentication for users.

100%

Comments: Authentication is enforced at the domain/user level, not at the Windows machine.

5.6.4 Enforces non-PIV, two-factor authentication for all users.

0%

5.6.5 Enforces two-factor PIV card for all users.

0%

Comments: SSA Windows machines are not configured to require a PIV card for authentication. This is handled at the user level.

5.7 Does the organization have a policy in place that requires the review of privileged network users' privileges? (If the answer is no, then answer 'N/A' for questions 5.7.1 through 5.7.2.)

Yes

5.7.1 What percentage of privileged network users had their privileges reviewed this year for the following?

5.7.1.1 Privileges on that account reconciled with work requirements.

1%

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

100%

Comments: The SSA Active Directory Domain Administrator role is the highest level of network access. This role is limited to a small number of employees within SSA's Office of Telecommunications and Systems Operations.

5.7.2 What percentage of privileged network users had their privileges adjusted or terminated after being reviewed this year?

Section 5: Identity and Access Management

30%

5.8 What percentage of the organizations systems that have intergovernmental users enforce two-factor PIV card authentication for all users? (Organizations with no intergovernmental systems may respond with N/A.)

0%

5.9 Does your organization's Federal Identity, Credential, and Access Management (FICAM) implementation plan include an enterprise Identity and Access Management approach that system owners can leverage to adopt PIV enablement?

Yes

Comments: SSA maintains application software and architecture configuration standards.

Section 6: Data Protection

6.1 What is the estimated number of hardware assets from 2.1 in each of the following mobile asset types, and how many are encrypted?

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 USG standards.

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 encryption of data on the device.
Laptop computers and netbooks	10901	10901
Tablet-type computers	0	0
BlackBerries and other smartphones	4192	4192
Other cellular devices	0	0
USB-connected devices (e.g., flash drives and removable hard drives)	0	0
Other mobile hardware assets (describe types in comments field)	0	0

6.2 What percentage of the organization's email traffic is on systems that implement FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to government organizations?

100%

Comments: Email encryption from point to point is dependent on both parties supporting encryption. SSA's devices support it. The recipients would also need to be configured for encryption.

6.2.1 What percentage of inter-organization email traffic is on systems that implement FIPS 140-2 compliant encryption technologies, such as S/MIME, PGP, OpenPGP, or PKI, when sending messages to the public?

100%

Section 6: Data Protection

Comments: Email encryption from point to point is dependent on both parties supporting encryption. SSA's devices support it. The recipients would also need to be configured for encryption.

- 6.3 Which one of the following best describes the organization's PKI Certificate Authority? Respond with the letter of that option. The organization**
- c. Receives PKI support from a Federal or commercial Shared Service Provider, but is responsible for some portion of the PKI service.**

Section 7: Boundary Protection

- 7.1 What percentage of the required TIC 2.0 Capabilities are implemented?**
96%
- 7.2 What percentage of external network traffic to/from the organization's networks passes through a TIC/MTIPS?**
100%
- 7.3 What percentage of external network/application interconnections to/from the organization's networks passes through a TIC/MTIPS?**
100%
- 7.4 What percentage of organization email systems implement sender verification (anti-spoofing) technologies when sending messages?**
100%
- 7.5 What percentage of organization email systems use sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network?**
100%
- 7.6 What is the estimated percentage of incoming email traffic (measured in messages) whose links or attachments are executed or opened in an in-line sandbox or virtual environment to ascertain whether or not they are malicious, and quarantined as appropriate, before they can be opened by the recipient? (Note: If you consider this to be infeasible, please explain why in the comments.)**
0%

Comments: SSA employs Microsoft's ForeFront for virus protection on Microsoft Exchange servers. All inbound mail is scanned before being delivered to recipient mailboxes. Viruses are eliminated as they are detected. SSA has also configured ForeFront to scan outbound mail, identify viruses, and eliminate them. SSA's ForeFront deployment is configured to update signature files on an hourly basis from Microsoft.

- 7.7 With what frequency does the organization conduct scheduled scans for unauthorized wireless access points (WAP) connected to an organizational network? Scans of different areas may count as different scans. A scan does not need to cover a particular percentage of the organization to be counted.**
0.25

Section 7: Boundary Protection

Comments: SSA WAPs have rogue access point detection and automated means for cataloguing identified access points which are automatically run 4 times daily.

- 7.7.1 What percentage of hardware assets in 2.1 are in facilities where scheduled WAP scans are conducted?
100%
- 7.7.2 How many WAPs were found?
17
- 7.8 With what frequency does the organization conduct planned, unannounced scans for unauthorized WAPs? Scans of different areas may count as different scans. A scan does not need to cover a substantial portion of the organization or assets to be counted.
0.25
- 7.8.1 What percentage of hardware assets in 2.1 are in facilities where planned, unannounced WAP scans are conducted?
100%
- 7.8.2 How many WAPs were found?
17
- 7.9 How many devices in 2.1, with DLP/DRM (Digital Loss Protection/Digital Rights Management), does the organization have at the gateway to capture outbound data leakage (e.g., PII)?
16
- 7.10 Is the organization's internet service (whether obtained through a TICAP or other means) configured to manage filters, excess capacity, bandwidth, or provide other redundancies to limit the effects of information-flooding types of denial-of-service attacks on the organization's internal networks and internet services. Such configuration may include agreements with external network operators to reduce the susceptibility to these types of attacks and respond to them.
Yes

Section 8: Incident Management

- 8.1 How many of the organization's hardware assets from 2.1 are on networks on which controlled network penetration testing was performed in the reporting period?
278266
- 8.1.1 What percentage of applicable events was detected by NOC/SOC during the penetration test?
0%
- 8.1.2 What percentage of applicable events was detected by NOC/SOC during the other scans or tests?
0%

Section 8: Incident Management

8.1.3 What was the mean time to detection of applicable events?

0.00

Section 9: Training and Education

9.1 What percentage of the organization's network users have been given and successfully completed cybersecurity awareness training in FY2013 (at least annually)?

97%

9.1.1 What is the estimated percentage of new users who satisfactorily completed security awareness training before being granted network access, or completed security awareness training within an organizationally defined time limit that provides 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 Users Receive Supplemental Cybersecurity Awareness Training
SSA	Quarterly

9.2.1 What was the average frequency in days of content provisions?

90.0

9.2.2 What percentage of this additional content that addresses emerging threats were not previously covered in the annual training?

100

9.2.3 What is the total number of organization-sponsored exercises (focusing on emerging threats such as phishing) designed to increase cybersecurity awareness and/or measure the effectiveness of cybersecurity awareness training in molding behavior?

8

9.2.4 What percentage of exercises in 9.2.3 suffered no problems or suffered problems that were addressed through appropriate training within three months?

100

9.3 How many of the organizations network users and other staff have significant security responsibilities?

585

9.3.1 What is the organization's standard for the longest acceptable amount of time between security training events for the personnel counted in question 9.3?

365

Section 9: Training and Education

- 9.3.2 How many of the personnel counted in question 9.3 have taken security training within the organizational standard defined in 9.3.1?
585

Section 10: Remote Access

- 10.1 How many people log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?
4835
- 10.2 For remote access, what percentage of people can log onto the organization's desktop LAN/WAN resources or services in each of the following ways?
- 10.2.1 Allowed to log on with user ID and password.
7%
- 10.2.2 Allowed, but not required, to log on with a non-PIV form of two-factor authentication.
0%
- Comments: SSA does not employ non-PIV two factor authentication for Windows.
- 10.2.3 Allowed, but not required, to log on with a two-factor PIV card.
0%
- 10.2.4 Required to log on with a non-PIV form of two-factor authentication.
0%
- Comments: SSA does not employ non-PIV two factor authentication for Windows.
- 10.2.5 Required to log on with a two-factor PIV card.
93%
- 10.2.6 Required to conduct PIV authentication at the user-account level.
93%
- Comments: All PIV user account level authentication occurs at network login.
- 10.3 What is the estimated percentage of remote access connections that have each of the following properties?
- 10.3.1 Utilizes FIPS 140-2-validated cryptographic modules.
100%
- 10.3.2 Prohibits split tunneling and/or dual-connected remote hosts where the laptop has two active connections.

Section 10: Remote Access

100%

10.3.3 Configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and require re-authentication to reestablish session.

100%

10.3.4 Scans for malware upon connection.

0%

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.

10.4 How many of the organizations systems are internet-accessible and are accessed by the organizations users? This excludes systems accessed through the remote access solutions covered in 10.1 and 10.2.

1

10.5 What percentage of organizations systems that are internet-accessible and are accessed by the D/A's users are configured for authentication in each of the following ways?

10.5.1 Allows user ID and password.

100%

10.5.2 Allows, but does not enforce, non-PIV two-factor authentication for users.

0%

10.5.3 Allows, but does not enforce, two-factor PIV card for users.

0%

10.5.4 Enforces non-PIV two-factor authentication for all users.

0%

10.5.5 Enforces two- factor PIV card for all users.

0%

Section 11: Network Security Protocols

11.1 How many public-facing domain names (second-level, e.g., www.dhs.gov) does the organization own? (Exclude domain names which host only FIPS-199 low-impact information on ISPs.)

4

11.1.1 How many DNS names from 11.1 are signed using DNSSEC?

Section 11: Network Security Protocols

3

11.1.2 What percentage of the second-level DNS names from 11.1 and their sub-domains are signed?

100%

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

100%

Inspector General

Section Report

2013

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 SP 800-53: CA-7).

Yes

1.1.2 Documented strategy and plans for continuous monitoring (NIST SP 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 SP 800-53, NIST 800-53A).

Yes

Comments:

We noted that the SSA continuous monitoring strategy includes manual control assessments and automated reporting mechanisms. Per the strategy, security controls currently selected for automated continuous monitoring are primarily technical controls that automated support tools can monitor and controls that may change frequently due to architectural or environment modifications such as updates and upgrades to hardware or software configurations. In regards to configuration standards, we noted that SSA made significant progress in developing baselines for authorized platforms in FY 2013; however, had not developed configuration baselines for all authorized platforms. In regards to vulnerability scanning capabilities, we noted the scanning tool used by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

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 a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A).

Yes

Comments:

We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per the continuous monitoring strategy, the successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

Section 1: Continuous Monitoring Management

- 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.

N/A

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

Comments:

We noted that while compartmentalized policies and procedures existed, SSA lacked a comprehensive Agency-wide policy and procedures related to application and system software change management including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results.

- 2.1.2 Defined standard baseline configurations.

Yes

Comments:

We noted that SSA established a list of authorized infrastructure software (platforms), had developed baselines for the majority of key platforms, and made significant progress in developing additional configuration baselines in FY 2013. However, it had not developed configuration baselines for all authorized platforms. Further, requirements associated with approval to deviate from agency security standards or configurations by submitting an exception request for software not on the authorized platform list were not in place during the entire fiscal year.

Section 2: Configuration Management

2.1.3 Assessments of compliance with baseline configurations.

Yes

Comments:

We noted the following regarding compliance with baseline configurations:

- Lack of configuration baselines for some platforms;
- Internal penetration testing identified high risk vulnerabilities due to unpatched software and misconfigurations, which resulted in testers obtaining domain administrative rights and access to the mainframe; and,
- Assessments of key configurations and access rights on significant platforms identified issues including misconfigurations.

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

No

Comments:

We noted that SSA had processes in place for remediation of results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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

No

Comments:

We noted that documentation for a significant number of deviations from the USGCB settings did not provide sufficient information pertaining to risk analysis and business justification for the deviation.

Section 2: Configuration Management

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

Yes

Comments:

We noted that while testing demonstrated that change management activities were occurring for both application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of change management processes conducted by the Agency. In addition, our testing identified system software weaknesses including completion of impact risk assessments, completion of test plans and retention of testing output, independent review of testing as well as validation changes were limited to those identified in the change request. For application changes, we noted instances where evidence to support testing and other requirements could not be provided. In addition, the Agency had not finalized and fully implemented controls associated with ensuring that mainframe privileged programs have been approved, can only be modified appropriately, and pose no security risks.

2.1.7 Process for timely and secure installation of software patches.

Yes

Comments:

We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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

No

Comments:

We noted the scanning tool used by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

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

No

Comments:

We noted that SSA had processes in place for remediation of scan results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results. In addition, misconfigurations were identified through testing of configurations on key platforms.

Section 2: Configuration Management

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

Yes

Comments:

We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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.

N/A

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 which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

Yes

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

Yes

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2).

Yes

Comments:

Although the Agency was able to identify all users, including contractors, with access to the mainframe and all employees with access to the network, SSA did not have an authoritative source / system(s) that identified and managed all contractors.

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

Yes

Comments:

We noted that SSA identified when special access requirements were necessary; however, we also noted that application developers had access to the production environment. These users did not obtain this access through the secondary ID process, which is a highly monitored process whereby programmers gain access to production for a limited time, and activity is subject to review.

Section 3: Identity and Access Management

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

Yes

3.1.5 Organization has 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 Organization has adequately planned for implementation of PIV for physical 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

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

No

Comments:

We identified numerous issues with logical access controls which resulted in inappropriate and / or unauthorized access including application developers (programmers) with unmonitored access to production and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

3.1.8 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:

The OIG Audit Report A-14-13-13050, *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network*, noted that while the Agency has a process to identify hardware devices connected to its network, we [the IG] determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA has processes to monitor the security level of connected devices, they were inconsistent with Agency policy in effect at the time of our [the IG] audit.

Section 3: Identity and Access Management

3.1.9 Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)

Yes

Comments: We noted that SSA was able to identify user and non-user accounts. However, we noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

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

No

Comments: We identified control failures related to the timely removal of logical access for terminated employees to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA employees and state Disability Determination Services employees. Additionally, SSA did not have an authoritative source that identified and managed all contractors and therefore was unable to support actual departure dates for contractors.

3.1.11 Identifies and controls use of shared accounts.

Yes

Comments: We noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

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.

N/A

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

Section 4: Incident Response and Reporting

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 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 SP 800-53, 800-61, and OMB M-07-16, M-06-19).

Yes

4.1.4 When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).

Yes

Comments:

We noted the incident reporting policy included information about reporting of incidents to law enforcement including but not limited to the OIG, Federal Protective Services and local law enforcement; however, the policy did not specify the established timeframes in which incidents should be reported to law enforcement.

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

Yes

Comments:

We noted that the SSA incident response procedures did not provide guidance or directives associated with establishing timeframes in which incidents should be resolved.

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 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; 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

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 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 SP 800-37, Rev.1.

Yes

Comments:

We noted that SSA had a comprehensive governance structure and organization-wide risk management strategy. However, we noted instances where off-site locations did not consistently apply SSA guidance such as requirements within the Program Operations Manual System.

5.1.3 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1.

Yes

5.1.4 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1.

Yes

5.1.5 Has an up-to-date system inventory.

Yes

5.1.6 Categorizes information systems in accordance with government policies.

Yes

5.1.7 Selects an appropriately tailored set of baseline security controls.

Yes

Section 5: Risk Management

5.1.8 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

5.1.9 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

5.1.10 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

5.1.11 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:

We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per SSA's continuous monitoring strategy, successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

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

Yes

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

Yes

5.1.14 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

Section 5: Risk Management

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

Yes

5.1.16 Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.

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.

N/A

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 SP 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

Comments:

We noted that SSA did not have an authoritative source / system(s) that identified and managed all contractors. Therefore, we were not able to gain reasonable assurance that the contractor population was complete. Without a complete population, the Agency may not be able to identify and track all contractors that require security awareness training. In addition, we noted that security training was not completed in a timely fashion for all employees and contractors (those that we were able to assess) or evidence to support completion of security training was not provided.

Section 6: Security Training

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 (NIST SP 800-50, 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

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

Yes

Comments:

We noted that although key activities associated with tracking and monitoring IT security weaknesses were being performed, Management had not fully documented a comprehensive policy and procedures covering all of the Agency's processes. Current policies and procedures associated with tracking of IT weaknesses, including the POA&M process, did not encompass the multiple tools and methods used by Management.

7.1.2 Tracks, prioritizes and remediates weaknesses.

Yes

Comments:

We noted instances where Information Technology security weaknesses were inadvertently "closed" within the Agency's tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

7.1.3 Ensures remediation plans are effective for correcting weaknesses.

Yes

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

7.1.4 Establishes and adheres to milestone remediation dates.

Yes

7.1.5 Ensures resources and ownership are provided for correcting weaknesses.

Yes

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and that require 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

Comments:

We noted instances where Information Technology (IT) security weaknesses were inadvertently “closed” within the Agency’s tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

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 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; 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

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 SP 800-53: AC-1, AC-17).

Yes

Section 8: Remote Access Management

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 SP 800-46, Section 4.2, Section 5.1).

Yes

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

Yes

Comments:

We noted that SSA's revised telework policy was in draft form pending resolution of administrative matters.

8.1.5 If applicable, multi-factor authentication is required for remote access (NIST SP 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 with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

Yes

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST SP 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 SP 800-53, PL-4).

Yes

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

Yes

Section 8: Remote Access Management

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

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

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 SP 800-53: CP-1).

Yes

9.1.2 The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (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:

We noted that SSA tested the majority of, but not all, major applications and/or general support systems as part of the disaster recovery exercise.

9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).

Yes

Section 9: Contingency Planning

9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

9.1.7 Testing or exercising of BCP and DRP 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 not 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 considers supply chain threats.

Yes

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? 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 a public cloud.

Yes

Section 10: Contractor Systems

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 (NIST SP 800-53: CA-2).

Yes

Comments:

We noted that while SSA management assessed the system security plan and planned for an independent assessment of controls for a contractor system, the assessment had not been executed prior to operation of the system.

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 a public cloud.

Yes

Comments:

We noted that the SSA contractor systems inventory did not include a service operated by a vendor. We noted that SSA had obtained a security controls assessment of this service.

10.1.4 The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 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

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

Yes

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.

N/A

Section 11: Security Capital Planning

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 SP 800-53: SA-2).**
Yes
- 11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).**
Yes
- 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

Senior Agency Official For Privacy

Section Report

2013
Annual
FISMA

Social Security Administration

Q1: Information Security Systems

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

Q2: PIAs and SORNs

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

Q3: Senior Agency Official for Privacy (SAOP) Responsibilities

- 3a** Can your organization demonstrate with documentation that the SAOP participates in all organization 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.

Q3: Senior Agency Official for Privacy (SAOP) Responsibilities

3b Can your organization 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 2013, the SAOP reviewed the Commerce Draft Bill on Consumer Data Privacy and the OMB Draft Memorandum on Guidance for Providing Administrative Data for Statistical Purposes.

3c Can your organization demonstrate with documentation that the SAOP participates in assessing the impact of the organization'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. The agency uses data loss prevention technology to mitigate the risk of PII disclosure via our communications systems. We also continue to participate in workgroups to assess the technological impact of social media and other emerging technologies.

Q4: Privacy Training

4a Does your organization 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:

See Tab B.

Q4: Privacy Training

- 4b** Does your organization 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:

See Tab B.

Q5: PIA and Web Privacy Policies and Processes

5a PIA Practices

- 5a(1)** Determining whether a PIA is needed

Yes

- 5a(2)** Conducting a PIA

Yes

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

Yes

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

Yes

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

Yes

- 5a(6)** Monitoring the organization'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)); it 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.

Q5: PIA and Web Privacy Policies and Processes

5b Web Privacy Practices

5b(1) Determining circumstances where the organization'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

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

Yes

Q6: 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	163	Y	X	X	102	153	49	X
TOTAL				3	163				102	153	49	

Q7: Written Privacy Complaints

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

6

7d Referrals — complaints referred to another organization with jurisdiction

0

Q8: Policy Compliance Review

Q8: Policy Compliance Review

8a Does the organization have current documentation demonstrating review of the organization'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 organization 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 organization use technologies that enable continuous auditing of compliance with stated privacy policies and practices?

Yes

Comments:

We use 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 organization coordinate with the organization'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.

Q9: SAOP Advice and Guidance

Q9: SAOP Advice and Guidance

9a Organization policies, orders, directives or guidance governing the organization'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 2013 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 organization'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.

Q9: 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.

Q10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking technologies")

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

Yes

Comments:

We use both Tier 1 (single session) and Tier 2 (multi-session without PII) web measurement and customization technologies, as defined in OMB Memorandum M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies.

10b Does the organization 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 2013 annual review.

10c Can the organization 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 organization 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 2013 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 and instead use the employee's personal identification number.



SOCIAL SECURITY

MEMORANDUM

Date: July 15, 2013

Refer To:

To: Peter D. Spencer
Deputy Commissioner
for Budget, Finance and Management

David F. Black
General Counsel
Senior Agency Official for Privacy

From: Kirsten J. Moncada
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) -- 2013 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 2013 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 either Anthony Tookes (6-0096) or Dave Lee (5-2848) of the Office of Privacy and Disclosure.

cc: Deputy Commissioner for Systems/Chief Information Officer (ODCS)

ADMINISTRATIVE INSTRUCTIONS MANUAL SYSTEM

MANUAL: General Administration

CHAPTER: 15 Personally Identifiable Information (PII) Loss and Remediation

INSTRUCTION NO.: 06

SUBJECT: Breach Notification Plan (BNP)

Audience: General (g)

Level: SSA

Date: 10/01/2013

INQUIRIES: Questions regarding the content of this issuance should be directed to [AOIS Controls@ssa.gov](mailto:AOIS.Controls@ssa.gov) in the Office of Systems (OS), Office of Information Security (OIS), 410-965-4859.

15.06.00 Table of Contents

- 15.06.01 [Purpose of Instruction](#)
- 15.06.02 [Authorities and References](#)
- 15.06.03 [Background](#)
- 15.06.04 [Scope](#)
- 15.06.05 [Policy](#)
- 15.06.06 [Is There Likely Risk of Harm? Factors to Consider](#)
- 15.06.07 [Factors to Determine the Risk of Harm](#)
- 15.06.08 [Whether Breach Notification Is Required](#)
- 15.06.09 [Content of Notification](#)
- 15.06.10 [SSA Official Responsible for Notification](#)
- 15.06.11 [How SSA Provides Notice](#)
- 15.06.12 [Attachment](#)

Attachment A. [Sample PII Breach Notification Letter](#)

15.06.01 [Purpose of Instruction](#)

- A. OMB [M-07-16](#) requirement applicable to all agencies: "Each agency should develop a breach notification policy and plan comprising the elements discussed in this Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification."
- B. The purpose of the Breach Notification Plan (BNP) is to establish a framework for when and how agencies will notify the subject of a harmful breach. The BNP and related procedures will ensure that SSA takes a consistent, reasonable approach to remediation and notification when there is a loss or suspected loss of PII. Publication of this AIMS guide codifies and supersedes all prior agency guidance.

15.06.02 [Authorities and References](#)

- A. [The Privacy Act of 1974](#) and related OMB Memorandums

- B. [OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007](#)
- C. [The E-Government Act of 2002 and Federal Information Security Management Act \(FISMA\) of 2002, 44 U.S.C. § 3541](#)
- D. [Information Systems Security Handbook \(ISSH\)](#)
- E. [National Institute of Standards and Technology \(NIST\) Special Publication 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#)
- F. [SSA Memo Dated 07/09/2013 - Designation of Deputy Commissioners \(DC\) to Issue Personally Identifiable Information \(PII\) Breach Notices](#)
- G. Related OMB Memorandums and NIST Guidelines

15.06.03 [Background](#)

[The Privacy Act](#), the [E-Government Act of 2002 \(including FISMA\)](#), and OMB guidelines, including [M-07-16](#), are the foundation of our BNP. Our BNP describes how we assess whether individuals are at risk of harm due to the breach, and whether we should provide notice of the breach to individuals and/or the public. The SSA BNP is distinct from OMB Guidance and our policy pertaining to reporting the loss of PII to management or to organizations such as the US Computer Emergency Response Team (US-CERT), which are covered by existing directives (see [AIMS, GAM 15.02](#)). The SSA BNP does not replace existing policy and procedure regarding security protocols and requirements for handling a security incident (see the [Information Systems Security Handbook \(ISSH\)](#)).

15.06.04 [Scope](#)

This policy is applicable agency-wide. It is one component of our comprehensive policies and procedures applicable to safeguarding information, implementing [Privacy Act](#) provisions, and responding to the loss of PII. The concept of the BNP is to use a best judgment standard, e.g., the sensitivity of a PII loss will be determined in context, to determine if risk of harm exists as a result of the breach. If risk of harm exists, notification may help individuals take steps to protect themselves from the consequences of the breach.

15.06.05 [Policy](#)

- A. The Deputy Commissioner or equivalent level official is responsible for ensuring that the component responds to the PII breach in accordance with this policy. The component that experiences the breach will work in consultation with the PII Breach Response Group (BRG). (See [AIMS, GAM 15.01.05](#).)
- B. SSA's BNP requires agency decision-makers to determine if a breach of PII puts an individual at risk of harm. To determine if we should notify affected individuals, the BNP requires us to consider the likely risk of harm and the level of impact. Our analysis of the likely risk of harm and the level of impact will determine when, what, how and who we should notify.
- C. If the breach involves an information system, SSA will follow existing procedures to take steps to mitigate further compromise of the system(s) involved in a breach. In addition to containing the breach, if circumstances warrant, we will take appropriate countermeasures, such as monitoring system(s) for misuse of the PII and for patterns of suspicious behavior. We also may consider whether we should give notice to the public at large.
- D. In deciding whether to provide notice, we should give greater weight to the likelihood that the PII is accessible and usable and to the likelihood that the breach may lead to harm. If we analyze the

factors (see [“Factors to Consider”](#) below) in a fact specific context, it is likely that we only will provide notification in instances where there is a likely risk of harm.

15.06.06 [Is There Likely Risk of Harm – Factors to Consider](#)

- A.** The decision-maker is to consider the specific facts, circumstances, and the context of the breach to evaluate the likely risk of harm and the level of impact on the individual(s). The decision-maker will use this information to determine whether notice should be given and to determine the nature and extent of the notice.
- B.** However, the fact that information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals. If information is properly protected (e.g., consistent with NIST standards and guides) the risk of compromise of the information may be low to non-existent.

15.06.07 [Factors that Determine the Risk of Harm](#)

A. Nature of the Data Elements Breached.

Identify the type of data breached. We consider the data elements in light of their context and the broad range of potential harms that may result from their potential use by unauthorized individuals.

B. Number of Individuals Affected.

The number of individuals affected is not determinative of the risk of harm. We will consider the number of affected individuals when determining the type or method(s) we use to provide notification.

C. Can an Unauthorized Person Access the Information?

We use NIST “Level of Impact” guidelines (see [Definitions, 15.01.08](#)) and consider answers to the questions below to assess the likelihood the breached information is accessible and will be used for malicious purposes.

1. Circumstances of the loss. How did the loss occur? Is the loss the result of a criminal act or is it likely to result in harm to the individual?
2. How easy or difficult is it to access the information in light of how the information is protected? For example, information on a protected (i.e., encrypted) device is less vulnerable than “hard copies” and unencrypted devices and files.
3. Is there evidence that the breached information is being used to harm the individual?
4. What is the likelihood unauthorized individuals will know the value of the information or sell it to others?

D. Can the Information Be Used to Cause Harm to Individuals?

1. **Broad Reach of Potential Harm.** [The Privacy Act](#) requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in “substantial harm, embarrassment, inconvenience, or unfairness” to any individual on whom information is maintained. SSA considers a number of possible harms associated with the breach of information:

- Economic Identity Theft;
- Medical Identity Theft;

- Theft;
- The effect of a breach of confidentiality on fiduciary responsibility;
- The potential for blackmail;
- The disclosure of private facts;
- Mental pain and emotional distress;
- Physical harm, e.g., disclosure of address information for victims of abuse;
- The potential for secondary uses of the information which could result in fear or uncertainty for the subject individuals; and/or
- The unwarranted exposure of information leading to humiliation or loss of self-esteem.

2. **Likelihood Harm Will Occur.** We ascertain if the type of information breached typically is used to cause harm to individuals. We may consult with law enforcement and/or the Office of the Inspector General (OIG) to assess the risk of harm to the individual.

After evaluating these factors, we review and reassess the level of impact (low, moderate or high) that previously we assigned to the information (see [15.06.07.C](#) above) using the NIST impact levels. The NIST impact levels (see [Definitions, 15.01.08](#)) will determine when and how we should provide notification.

15.06.08 [Whether Breach Notification Is Required](#)

In situations when there is little or no risk of harm, we generally will not issue notice. When the risk of harm is low, we also will consider the costs to individual and businesses, e.g., financial institutions, associated with responding to notices.

- When:** When warranted, we give notice without unreasonable delay (no later than 45 calendar days from the date of the PII incident report).” Permissible delays are limited only to those situations that involve law enforcement or national security considerations, or the need to restore the integrity of information systems prior to notification. Decisions to delay notification will be made by the Commissioner of Social Security (COSS) or his/her designee.
- Who and How:** We decide how to provide notice based on the number of people affected and the urgency with which they need to receive notice. We describe below the types of notice we may use exclusively or in combination. In general, breach notifications to individuals will be by letter or by telephone and we will use public notification in the event of a large scale (regional or national) breach.

We determine if we need to notify any third parties; e.g., those with oversight responsibilities, other agencies that may be affected by the breach and/or that may help mitigate the breach, the public, and/or the media.

15.06.09 [Content of Notification](#)

- A. We will use plain language. We will include the following information in all our breach notification materials, regardless of the medium or method.
- B. An apology;

- C. A brief description of what happened, including the date(s) of the breach and the date that we discovered it;
- D. A description of the types of PII involved in the breach (e.g., full name, Social Security number, date of birth, home address, disability information);
- E. A statement whether the information is protected;
- F. What steps individuals might wish to take to protect themselves from potential harm;
- G. What we are doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- H. Who affected individuals should contact for more information, which may include a toll-free telephone number, and/or postal address.

15.06.10 SSA Official Responsible for Notification

- A. The COSS or his/her designee will sign the written notices that we send to individuals. See AIMS GAM 15.06.02.F Notification must be compliant with Section 508 of the Rehabilitation Act. The law may require us to establish a Telecommunications Device for the Deaf (TDD) and/or to post a large print notice on the Agency's web site.
- B. If the breach involves a Federal contractor or a public-private partnership operating a system of records on our behalf, we will determine who is responsible for notification and ensure that corrective actions are taken. We include appropriate Federal Acquisition Regulation language regarding Federal Information Security Management Act requirements and PII loss reporting responsibilities in all contracts and other acquisition documents.

15.06.11 How SSA Provides Notice

As stated in 15.06.08, in general breach notifications to individuals will be by letter or by telephone. The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notices that we may use.

NOTE: The Office of Communications, the Office of Legislative and Congressional Relations and Office of General Counsel/Office of Privacy and Disclosure must be consulted when preparing a notice (other than the one in Attachment A); likewise any component considering web posting, existing government wide services, newspapers or other public media outlets or substitute notice must confer with these offices as part of the development of the product.

- A. **Telephone:** Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected.
- B. **First-Class Mail:** We will provide written notice by first-class mail. We will send the notice separately from other SSA mailings so that it is obvious to the recipient that it pertains to SSA and that the matter is urgent.
- C. **E-Mail:** We may use e-mail notification exclusively only if the individual has provided an e-mail address to us and expressly has given his or her consent to use e-mail as the primary means of communication with us. We may use e-mail in conjunction with written notice if the circumstances of the breach warrant such an approach. E-mail notification may include links to the Agency and <http://www.usa.gov> web sites, where the notice may be "layered" so that the most important summary facts are up front with additional information provided under link headings.

- D. Web Posting:** Depending on the circumstances, we may post information about the breach and notification on our home page. The posting may include a link to Frequently Asked Questions (FAQs) and other information to assist the public's understanding of the breach and of the notification process. The information also may appear on the <http://www.usa.gov/> web site. We may consult with the General Services Administration's (GSA) USA Services regarding using their call center.
- E. Existing Government Wide Services:** We may consider Government-wide services already in place to provide support services such as USA Services, including 1-800-FedInfo and <http://www.usa.gov/>.
- F. Newspapers or other Public Media Outlets:** In rare circumstances, we may supplement individual notices with notifications in newspapers or other public media outlets. We may use toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.
- G. Substitute Notice:** We may use substitute notice in those instances where we do not have sufficient contact information to provide another means of notification. Substitute notice may consist of a conspicuous posting of the notice on the home page of our web site and/or notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media may include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

15.06.12 [Attachment](#)

Attachment A. [Sample PII Breach Notification Letter](#)

Attachment A. (GAM 15.06) Sample PII Breach Notification Letter

Social Security Administration
Important Information

Date:

NAME
MAILING ADDRESS
CITY ST ZIPCODE

We regret to inform you that on (1) _____, (2) _____
_____. The (3) _____
_____ contained personally identifiable information about you including your (4) _____,
_____, and _____.

(The above paragraph needs to be very specific in explaining the circumstances of the breach and what PII was compromised)

We apologize for any inconvenience or concern this incident may cause you. In this notice, we tell you what steps you may wish to consider taking to protect yourself, especially if you have any reason to believe that someone is using your personal information.

(In addition, if a crime was involved (i.e. stolen laptop), and the OIG is involved, the following language should be inserted:)

Social Security's Office of the Inspector General is working closely with appropriate law enforcement authorities to investigate this matter.

What Steps You Can Take For Your Protection

- To learn about precautions you can take, please read the enclosed leaflet "Identity Theft and Your Social Security Number."
- If you have reason to believe that someone is using your personal information, including your Social Security number, you should contact the Federal Trade Commission at 1-877-438-4338 or at www.ftc.gov/bcp/edu/microsites/idtheft/.

If You Have Any Questions

If you have any questions, please call us at (5) _____. We can answer most questions over the phone. If you do call, please have this letter with you; it will help us answer your questions. You can also e-mail your questions to (6) _____ or write us at the address shown at the top of this letter. For your own protection, you should not include your Social Security number on any e-mail correspondence.

Our Sincere Apology

The men and women of the Social Security Administration take our obligation to protect the integrity and privacy of your Social Security records very seriously. Please accept our sincere apology for any inconvenience or concern this situation may cause you. We are committed to ensuring that instances such as this do not occur in the future.

Appropriate Deputy Commissioner or Regional Commissioner

FILL-IN INFORMATION

1. *Date of breach*
2. *Describe the breach, including what was lost and how it was lost. For example:*
 - Hearing-related documents were stolen from an employee's vehicle.
 - A laptop computer was stolen from an employee's office.
 - A notice addressed to you was accidentally mailed to someone else's address
3. *Describe whatever was lost or compromised. For example:*
 - Laptop computer
 - Claims file
 - List of social security numbers
4. *List the types of data that were breached. For example:*

Full name, Social Security number, date of birth, home address, and medical records...
5. *Telephone number and times of service. While it could be local SSA office information, we expect the fill-in language will be the national 800 number in most cases:*

1-800-772-1213 (TTY 1-800-325-0778) between 7:00 a.m. and 7:00 p.m., Monday through Friday.
6. *E-mail address of the notifying component, if appropriate for the component.*

OIG

Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's
Compliance with the Federal
Information Security Management
Act of 2002 for Fiscal Year 2013

A-14-13-13086 | November 2013

MEMORANDUM

Date: November 26, 2013

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 2013 (A-14-13-13086)

The attached final report summarizes Grant Thornton, LLP's, (Grant Thornton) Fiscal Year (FY) 2013 audit of the Social Security Administration's (SSA) information security program and practices, as required by Title III of the *E-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 we, or an independent external auditor, as determined by the Inspector General (IG), perform an annual evaluation that includes

- testing the effectiveness of SSA's information security policies, procedures, and practices of a representative subset of the agency's information systems and
- assessing compliance with FISMA requirements, and related information security policies, procedures, standards, and guidelines.

Under a contract we monitored, Grant Thornton, an independent certified public accounting firm, audited SSA's compliance with FISMA for FY 2013. Grant Thornton's report, along with its responses to the FY 2013 IG FISMA reporting metrics developed by the Department of Homeland Security (DHS), are submitted through CyberScope pursuant to Office of Management and Budget (OMB) Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

Objective, Scope, and Methodology

The objective of Grant Thornton's audit was to determine whether SSA's overall information security program and practices were effective and consistent with the FISMA requirements, as defined by DHS. In addition to FISMA and DHS' guidance, Grant Thornton tested SSA's overall information security program and practices using guidance from OMB and the National Institute of Standards and Technology, as well as SSA policy.

Grant Thornton conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Grant Thornton plan and perform

the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives.

Audit Results

For FY 2013, Grant Thornton determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. However, weaknesses identified limited the overall program's effectiveness in adequately protecting the Agency's information and information systems. Grant Thornton concluded that each of the metrics was generally consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology standards; however, Grant Thornton identified weaknesses in the following metrics:

Continuous Monitoring Management	Configuration Management	Identity and Access Management	Incident Response and Reporting	Risk Management
Security Training	Plan of Action & Milestones	Remote Access Management	Contingency Planning	Contractor Systems Oversight

Weaknesses in Sections 2, *Configuration Management* and 3, *Identity and Access Management*, resulted in negative conclusions to components of these metrics. For FY 2013, Grant Thornton concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a **significant deficiency** under FISMA.

OIG Evaluation of Grant Thornton's Audit Performance

To fulfill our responsibilities under the *Inspector General Act of 1978*, we monitored Grant Thornton's audit of SSA's FY 2013 compliance with FISMA by

- reviewing Grant Thornton's audit approach and planning;
- evaluating its auditors qualifications and independence;
- monitoring the audit progress;
- examining Grant Thornton's work papers;
- reviewing Grant Thornton's audit report to ensure compliance with Government Auditing Standards;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

Page 3 – The Commissioner

Grant Thornton is responsible for the attached auditor's report and the work and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton's performance under the terms of the contract. Our monitoring review, as described above, disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

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.

A handwritten signature in black ink, appearing to read "Pat O'Carroll Jr.", written in a cursive style.

Patrick P. O'Carroll, Jr.

Attachment



MEMORANDUM

Date: November 26, 2013
To: SSA Office of the Inspector General
From: Grant Thornton, LLP
Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013 (A-14-13-13086)

In conjunction with the audit of the Social Security Administration's (SSA) Fiscal Year (FY) 2013 Financial Statements, the Office of the Inspector General engaged us to conduct the performance audit on SSA's compliance with *Federal Information Security Management Act of 2002* (FISMA) for FY 2013. The objective was to determine whether SSA's overall information security program and practices were effective and consistent with the requirements of the FISMA as defined by the Department of Homeland Security. We are pleased to report the results of our audit and appreciate the support provided to us in completing this review.

Our report is intended solely for the information and use of management at SSA, SSA's Office of the Inspector General, the Office of Management and Budget, the Government Accountability Office, and Congress and is not intended to be and should not be used by anyone other than these specified parties.

Grant Thornton LLP

Alexandria, Virginia
November 26, 2013

The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013

November 2013

Report Summary

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

SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year 2013 FISMA performance audit in accordance with *Government Auditing Standards* commonly referred to as the "Yellow Book" which sets forth generally accepted government auditing standards. We assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and through performance of additional testing procedures as needed. We determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and other applicable regulations, standards, and guidance applicable during the audit period.

Our Findings

We determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. 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. We concluded that these weaknesses constituted a significant deficiency under FISMA.

Our Recommendations

- Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze current access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.
- Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.
- Address weaknesses identified within the comments of Appendix B by implementing our recommendations provided throughout the audit in our Notices of Finding and Recommendation.

TABLE OF CONTENTS

Objective	1
Background	1
Scope and Methodology	1
Results of Review	2
Agency Efforts to Resolve Weaknesses and Potential Cause for the FY 2013 FISMA Significant Deficiency	7
Conclusions and Recommendations	7
Views of Responsible Officials	8
Appendix A – Scope and Methodology	A-1
Appendix B – Response to Fiscal Year 2013 Inspector General <i>Federal Information Security Management Act</i> Reporting Metrics	B-1
Appendix C – The Social Security Administration’s General Support Systems and Major Applications	C-1
Appendix D – Metrics Defined	D-1
Appendix E – Major Contributors.....	E-1

ABBREVIATIONS

DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards Publication
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FSA	Financial Statement Audit
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAS	Government Auditing Standards
Grant Thornton	Grant Thornton LLP
IG	Inspector General
IT	Information Technology
NFR	Notice of Finding and Recommendation
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
SSA	Social Security Administration
U.S.C.	United States Code

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).

To achieve this objective, we assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems. We then determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and other regulations, standards, and guidance applicable during the audit period.

BACKGROUND

In conjunction with the audit of SSA's Fiscal Year (FY) 2013 Financial Statements,¹ SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the FY 2013 FISMA performance audit. FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002), includes the following key requirements:

- Each agency must develop, document, and implement an agency-wide information security program.²
- 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.³
- The agency's Inspector General (IG), or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.⁴

SCOPE AND METHODOLOGY

On November 30, 2012, DHS issued reporting metrics for the IG's FY 2013 FISMA submission. We audited the following 11 reporting metrics as part of our review:

¹ Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009.

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

³ Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A); 44 U.S.C. § 3544(a)(1)(A).

⁴ 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).

FY 2013 Inspector General FISMA Reporting Metrics

- Continuous Monitoring Management
- Configuration Management
- Identity and Access Management
- Incident Response and Reporting
- Risk Management
- Security Training
- Plan of Action & Milestones (POA&M)
- Remote Access Management
- Contingency Planning
- Contractor Systems
- Security Capital Planning

The FY 2013 SSA FISMA performance audit was performed in accordance with *Government Auditing Standards* (GAS), issued by the Comptroller General of the United States, also known as the “Yellow Book” which sets forth generally accepted government auditing standards (GAGAS). We followed the Federal Information System Controls Audit Manual (FISCAM), which provides guidance for evaluating Electronic Data Processing general, and application controls in a Federal audit under GAGAS. In accordance with standards contained in GAS issued by the Comptroller General of the United States, we leveraged work performed as part of the FY 2013 Financial Statement Audit (FSA) and performed additional procedures as required to assess the reporting metrics listed above.

This report informs Congress and the public about SSA’s security performance and fulfills the Office of Management and Budget (OMB) and DHS requirements under FISMA to submit an annual report to Congress. Refer to Appendix A for additional information on our scope and methodology.

RESULTS OF REVIEW

For FY 2013, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements.⁵ However, weaknesses identified limited the overall program’s effectiveness to adequately protect the Agency’s information and information systems. We concluded that each of the metrics was generally

⁵ Our conclusion was based on our assessment of SSA’s compliance with DHS’ *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. 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 various issues in our assessment that are documented in the comments within Appendix B.

consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology (NIST) standards; however, we identified weaknesses in the following metrics:

Continuous Monitoring Management	Configuration Management	Identity and Access Management	Incident Response and Reporting	Risk Management
Security Training	POA&M	Remote Access Management	Contingency Planning	Contractor Systems Oversight

Refer to Appendix D for additional information on metrics.

Weaknesses in Section 2, *Configuration Management* and Section 3, *Identity and Access Management*, resulted in negative conclusions to the following metrics:

Configuration Management

- 2.1.4 – Process for timely (as specified in organization policy or standards) remediation of scan result deviations.
- 2.1.5 - For Windows-based components, United States Government Configuration Baselines (USGCB) secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.
- 2.1.8 - Software assessing (scanning) capabilities are fully implemented.
- 2.1.9 - Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

Identity and Access Management

- 3.1.7 – Ensures that the users are granted access based on needs and separation-of-duties principles.
- 3.1.10 – Ensures that accounts are terminated or deactivated once access is no longer required.

We provided comments on these key components of SSA's information security program to Management throughout the audit.⁶ Refer to Appendix B for additional information on these and other weaknesses and conclusions.

We assessed the significance of these weaknesses individually and in the aggregate to determine the risk to SSA's overall information systems security program and management's control structure. We noted that while all these findings, in aggregate, impacted risk, the following weaknesses had the most significant impact on our conclusion:

- *Lack of a comprehensive Agency-wide policy and procedures related to vulnerability management, including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure/validation* - During internal penetration testing, we were able to take advantage of software vulnerabilities, misconfigurations, and restricted information to assume control of two servers, the Windows domain, as well as, gaining access to the mainframe without detection. This is the third successive year we have gained control of the SSA Windows system without detection. During subsequent assessments of the Agency's overall vulnerability management process, we noted that a key scanning tool was not being fully used to identify vulnerabilities across SSA's network, and Agency-wide comprehensive policies and procedures on vulnerability management were not established.

The Agency corrected the specific software vulnerabilities identified during our penetration testing, developed configuration standards for the software, and began using more capabilities of the scanning tool. However, without a comprehensive process in place, security threats may not be appropriately prioritized and remediated.

- *Lack of comprehensive Agency-wide policy and procedures related to management of application and system software changes, including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results* – While our testing demonstrated that change management activities were occurring for application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of the change management processes conducted by the Agency. Our testing noted the following.
 - System Software - An impact/risk assessment to determine the security implications for mainframe changes did not occur. Further, for the majority of changes tested, we noted that developers were responsible for testing their own changes and implementing these changes into production. While management performed a review to validate that updates made were associated with an approved change, there were no requirements nor guidance related to the types of testing to be performed (including security reviews), nor for retention or

⁶ We provided Agency management with a Notice of Finding and Recommendation (NFR) for each individual weakness. The NFR included the condition, criteria, cause, effect, and recommendation.

independent review of testing documentation, nor validation that the change made was limited to the requirements in the approved change ticket.

- Application Changes - We noted instances where evidence to support testing and other requirements could not be provided.

These issues increase the risk that changes to applications and supporting system software, which may impact benefit claim processing, payments, or financial data, do not function as intended or introduce security risks.

- *Lack of controls related to the identification and monitoring of high-risk programs operating on the mainframe⁷* - The Agency had not finalized and fully implemented controls associated with ensuring that privileged programs had been approved, could only be modified appropriately, and posed no security risks. Management continues making control enhancements including, but not limited to, identifying privileged programs, the review of privileged programs from a security perspective, access restrictions to all privileged programs, and change/monitoring control enhancements.

Without appropriate controls, there is an increased risk that the security posture and controls may be bypassed or compromised.

- *Access control issues* - Our testing identified numerous issues with logical access controls that are in place to mitigate the risk of unauthorized access. Our testing identified the following issues:
 - Access Authorization - Our testing identified control failures related to the appropriate completion of authorization forms. Included in these control failures were new hires, transferred employees, and contractors.
 - Access Removal - Our testing identified control failures related to the timely removal of terminated employees' logical access to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA and State Disability Determination Services employees who retained access after they were terminated. Additionally, SSA did not have an authoritative source to identify and manage all contractors and therefore SSA was unable to supply actual departure dates for contractors to substantiate timely removal of access.

⁷ 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.

- Profile⁸ Content and Analysis Review Program and Supporting Profile Controls - SSA Management continues to make progress in assessing profile content to validate that profiles only provide access to the minimal resources required for users to complete job functions. However, SSA had not completed the review of all profiles that are relevant to critical applications and supporting systems nor had SSA completed other profile quality initiatives including, but not limited to, some control enhancements.

As a result of these deficiencies, we noted numerous issues of unauthorized and inappropriate access including application developers (programmers) with unmonitored access to production data and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

For FY 2013, we concluded that the risk and severity of SSA's information security weaknesses, including those highlighted above and other weaknesses outlined in Appendix B, 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.⁹

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.”¹⁰

These security deficiencies, when aggregated, created a weakness in SSA's overall information systems security program that we concluded significantly compromised the security of its information and information systems.

⁸ 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.

⁹ **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).

¹⁰ OMB, M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013, page 8.

Agency Efforts to Resolve Weaknesses and Potential Cause for the FY 2013 FISMA Significant Deficiency

In response to the FY 2012 material weakness in information systems controls reported within the internal controls opinion¹¹ and FY 2012 FISMA significant deficiency,¹² SSA developed functional remediation teams to investigate issues, identify root causes, and implement corrective actions. Each functional remediation team, with oversight from SSA leadership, took risk-based approaches to remediation—addressing higher risk areas immediately, and planning for future security enhancements. Management’s risk based approach included correction of vulnerabilities identified through our specific tests as well as development and implementation of institutionalized and repeatable processes to prevent future weaknesses.

While SSA made significant efforts to strengthen controls over its systems and address weaknesses, our FY 2013 testing continued to identify general control issues in both design and operation of key controls. We believe that in many cases these deficiencies continue to exist because of one or a combination of the following:

- Control enhancements and newly designed controls require additional time to effectuate throughout the environment;
- By focusing resources on higher risk weaknesses, SSA was unable to implement corrective action for all aspects of the prior year issues; and/or,
- The design and/or operational effectiveness of enhanced or newly designed controls did not completely address risks.

SSA continues to implement corrective actions to address remaining deficiencies, which in many cases, is a continuation of previously established risk based strategies.

CONCLUSIONS AND RECOMMENDATIONS

For FY 2013, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. 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. We noted weaknesses within Section 2, *Configuration Management*, and Section 3, *Identity and Access Management*, that resulted in negative answers to metrics and various other issues that resulted in comments to the FISMA metrics located in Appendix B. Based on these factors, we concluded that these weaknesses constituted a significant deficiency under FISMA.

¹¹ Grant Thornton, *Independent Auditor’s Report* on the audit of SSA’s FY 2012 financial statements, November 8, 2012.

¹² SSA OIG, *The Social Security Administration’s Compliance with the Federal Information Security Management Act of 2002 for the Fiscal year 2012*, (A-14-12-12120), November 15, 2012.

SSA needs to 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.

To mitigate the risks of the issues noted in the significant deficiency, management should consider the following:

- Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze current access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.
- Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.
- Address weaknesses identified within the comments of Appendix B by implementing our recommendations provided throughout the audit in our Notices of Finding and Recommendation.

VIEWS OF RESPONSIBLE OFFICIALS

Our conclusions were discussed with SSA responsible officials who generally agreed with our findings and recommendations. SSA's official responses will be included in their comments to the independent auditor's report on the audit of SSA's FY 2013 financial statements.¹³

¹³ Grant Thornton, *Independent Auditor's Report* on SSA's FY 2013 financial statements will be released in December 2013.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency’s Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency’s information security programs and practices, as well as a review of an appropriate subset of agency systems.¹ The Social Security Administration’s (SSA) IG contracted with us, Grant Thornton LLP (Grant Thornton), to audit the SSA’s Fiscal Year (FY) 2013 financial statements.² Because of the extensive internal control system work that is completed as part of that audit, the FISMA review requirements were incorporated into our financial statement audit (FSA) contract. To maximize efficiencies and minimize the impact to SSA management during the FISMA performance audit, we used Appendix IX – *Application of FISCAM to FISMA* from the GAO *Federal Information System Controls Audit Manual* (FISCAM) in order to leverage testing performed during the SSA FSA. Additionally, governed by the 2011 *Government Audit Standards* Chapters 1 through 3, 6, and 7 – in particular Chapter 6, *Field Work Standards for Performance Audits - Using the Work of Others*, we leveraged the information technology general controls testing performed during the FSA wherever it was deemed appropriate. In some cases, FISMA tests were unique from those of the FSA; therefore, we designed test procedures to deliver adequate coverage over those unique areas.

Testing was performed in accordance with specific criteria as promulgated by the following:

- FISMA law;
- Office of Management and Budget (OMB) guidance;
- Department of Homeland Security (DHS) annual FISMA reporting instructions and annual FISMA IG reporting metrics, OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources;
- Standards and guidelines issued by the National Institute of Standards and Technology (NIST) – including, NIST Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*;
- Federal Information Processing Standards Publication (FIPS) - 199, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS-200 *Minimum Security Requirements for Federal Information and Information Systems*, FIPS- 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;

¹ Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(1), (a)(2)(A), (a)(2)(B); and (b)(1), 44 U.S.C. §§ 3545(a)(1) (a)(2)(A), (a)(2)(B); and (b)(1).

² Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009.

- Federal Information Security Memorandum 13-01, *FY 2013 Metrics for the Federal Information Security Management Act and Agency Privacy Management Act and Operational Reporting Instructions*;
- Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics; and,
- Local SSA policies.

Our assessment followed the DHS FY 2013 FISMA guidance³ 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 conducted this audit in accordance with generally accepted government auditing standards. These standards required 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 the audit objectives.

³ DHS Federal Information Security Memorandum 13-01, *FY 2013 Metrics for the Federal Information Security Management Act and Agency Privacy Management Act and Operational Reporting Instructions*, September 2013.

Appendix B – RESPONSE TO FISCAL YEAR 2013 INSPECTOR GENERAL *FEDERAL INFORMATION SECURITY MANAGEMENT ACT* REPORTING METRICS

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 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 SP 800-53, 800-53A). (AP)**

FY2013 Conclusion: Yes

Comments: We noted that the SSA continuous monitoring strategy includes manual control assessments and automated reporting mechanisms. Per the strategy, security controls currently selected for automated continuous monitoring are primarily technical controls that automated support tools can monitor and controls that may change frequently due to architectural or environment modifications such as updates and upgrades to hardware or software configurations. In regards to configuration standards, we noted that SSA made significant progress in developing baselines for authorized platforms in FY 2013; however, had not developed configuration baselines for all authorized platforms. In regards to vulnerability scanning capabilities, we noted the scanning tool used

by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

- 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 a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). (AP)**

FY2013 Conclusion: Yes

Comments: We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per the continuous monitoring strategy, the successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

- 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: N/A

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?**

FY2013 Conclusion: Yes

- 2.1.1. Documented policies and procedures for configuration management. (Base)**

FY2013 Conclusion: Yes

Comments: We noted that while compartmentalized policies and procedures existed, SSA lacked a comprehensive Agency-wide policy and procedures related to application and system software change management including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results.

- 2.1.2. Defined standard baseline configurations. (Base)**

FY2013 Conclusion: Yes

Comments: We noted that SSA established a list of authorized infrastructure software (platforms), had developed baselines for the majority of key platforms, and made significant progress in developing additional configuration baselines in FY 2013. However, it had not developed configuration baselines for all authorized platforms. Further, requirements associated with approval to deviate from agency security standards or configurations by submitting an exception request for software not on the authorized platform list were not in place during the entire fiscal year.

2.1.3. Assessments of compliance with baseline configurations. (Base)

FY2013 Conclusion: Yes

Comments: We noted the following regarding compliance with baseline configurations:

- Lack of configuration baselines for some platforms;
- Internal penetration testing identified high risk vulnerabilities due to unpatched software and misconfigurations, which resulted in testers obtaining domain administrative rights and access to the mainframe; and,
- Assessments of key configurations and access rights on significant platforms identified issues including misconfigurations.

2.1.4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations. (Base)

FY2013 Conclusion: No

Comments: We noted that SSA had processes in place for remediation of results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

2.1.5. For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. (Base)

FY2013 Conclusion: No

Comments: We noted that documentation for a significant number of deviations from the USGCB settings did not provide sufficient information pertaining to risk analysis and business justification for the deviation.

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

FY2013 Conclusion: Yes

Comments: We noted that while testing demonstrated that change management activities were occurring for both application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of change management processes conducted by the Agency. In addition, our testing identified system software weaknesses including completion of impact risk assessments, completion of test plans and retention of testing output, independent review of testing as well as validation changes were limited to those identified in the change request. For application changes, we noted instances where evidence to support testing and other requirements could not be provided.

In addition, the Agency had not finalized and fully implemented controls associated with ensuring that mainframe privileged programs have been approved, can only be modified appropriately, and pose no security risks.

2.1.7. Process for timely and secure installation of software patches. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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

FY2013 Conclusion: No

Comments: We noted the scanning tool used by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

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

FY2013 Conclusion: No

Comments: We noted that SSA had processes in place for remediation of scan results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be

remediated timely as demonstrated by internal penetration testing results. In addition, misconfigurations were identified through testing of configurations on key platforms.

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

FY2013 Conclusion: Yes

Comments: We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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: N/A

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 which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). (Base)

FY2013 Conclusion: Yes

Comments: Although the Agency was able to identify all users, including contractors, with access to the mainframe and all employees with access to the

network, SSA did not have an authoritative source / system(s) that identified and managed all contractors.

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

FY2013 Conclusion: Yes

Comments: We noted that SSA identified when special access requirements were necessary; however, we also noted that application developers had access to the production environment. These users did not obtain this access through the secondary ID process, which is a highly monitored process whereby programmers gain access to production for a limited time, and activity is subject to review.

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

FY2013 Conclusion: Yes

Comments: N/A

3.1.5. Organization has 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). (AP)

FY2013 Conclusion: Yes

Comments: N/A

3.1.6. Organization has adequately planned for implementation of PIV for physical 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).

FY2013 Conclusion: Yes

Comments: N/A

3.1.7. Ensures that the users are granted access based on needs and separation-of-duties principles. (Base)

FY2013 Conclusion: No

Comments: We identified numerous issues with logical access controls which resulted in inappropriate and / or unauthorized access including application developers (programmers) with unmonitored access to production and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

3.1.8. 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.) (Base)

FY2013 Conclusion: Yes

Comments: The OIG Audit Report A-14-13-13050, *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network*, noted that while the Agency has a process to identify hardware devices connected to its network, we [the IG] determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA has processes to monitor the security level of connected devices, they were inconsistent with Agency policy in effect at the time of our [the IG] audit.

3.1.9. Identifies all user and non-user accounts (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users) (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA was able to identify user and non-user accounts. However, we noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

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

FY2013 Conclusion: No

Comments: We identified control failures related to the timely removal of logical access for terminated employees to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA employees and state Disability Determination Services employees. Additionally, SSA did not have an authoritative source that identified and managed all contractors and therefore was unable to support actual departure dates for contractors.

3.1.11. Identifies and controls use of shared accounts. (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of

requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

- 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: N/A

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 4.1.2. Comprehensive analysis, validation and documentation of incidents. (KFM)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 4.1.4. When applicable, reports to law enforcement within established timeframes (SP 800-61). (KFM)**

FY2013 Conclusion: Yes

Comments: We noted the incident reporting policy included information about reporting of incidents to law enforcement including but not limited to the OIG, Federal Protective Services and local law enforcement; however, the policy did

not specify the established timeframes in which incidents should be reported to law enforcement.

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

FY2013 Conclusion: Yes

Comments: We noted that the SSA incident response procedures did not provide guidance or directives associated with establishing timeframes in which incidents should be resolved.

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

FY2013 Conclusion: Yes

Comments: N/A

4.1.7. Is capable of correlating incidents. (Base)

FY2013 Conclusion: Yes

Comments: N/A

4.1.8. Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA had a comprehensive governance structure and organization-wide risk management strategy. However, we noted instances where off-site locations did not consistently apply SSA guidance such as requirements within the Program Operations Manual System.

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.5. Has an up-to-date system inventory. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.6. Categorizes information systems in accordance with government policies. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.7. Selects an appropriately tailored set of baseline security controls. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.9. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.10. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.11. 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. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per SSA's continuous monitoring strategy, successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.13. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.14. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.16. Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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: N/A

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?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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. (KFM)

FY2013 Conclusion: Yes

Comments: We noted that SSA did not have an authoritative source / system(s) that identified and managed all contractors. Therefore, we were not able to gain reasonable assurance that the contractor population was complete. Without a complete population, the Agency may not be able to identify and track all contractors that require security awareness training. In addition, we noted that security training was not completed in a timely fashion for all employees and contractors (those that we were able to assess) or evidence to support completion of security training was not provided.

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. (KFM)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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?

FY2013 Conclusion: Yes

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. (Base)

FY2013 Conclusion: Yes

Comments: We noted that although key activities associated with tracking and monitoring IT security weaknesses were being performed, Management had not fully documented a comprehensive policy and procedures covering all of the Agency's processes. Current policies and procedures associated with tracking of IT weaknesses, including the POA&M process, did not encompass the multiple tools and methods used by Management.

7.1.2. Tracks, prioritizes and remediates weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where Information Technology security weaknesses were inadvertently "closed" within the Agency's tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

7.1.3. Ensures remediation plans are effective for correcting weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.4. Establishes and adheres to milestone remediation dates. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.5. Ensures resources and ownership are provided for correcting weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where Information Technology (IT) security weaknesses were inadvertently “closed” within the Agency’s tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

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

FY2013 Conclusion: Yes

Comments: N/A

7.1.8. Program officials 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; OMB M-04-25). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 8.1.2. Protects against unauthorized connections or subversion of authorized connections. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 8.1.4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)**

FY2013 Conclusion: Yes

Comments: We noted that SSA's revised telework policy was in draft form pending resolution of administrative matters.

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

FY2013 Conclusion: Yes

Comments: N/A

8.1.6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

8.1.8. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: N/A

8.3. Does the organization have a policy to detect and remove unauthorized (rogue) connections?

FY 2013 Conclusion: Yes

Comments: 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?

FY2013 Conclusion: 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 SP 800-53: CP-1). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.2. The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

9.1.4. Testing of system specific contingency plans. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA tested the majority of, but not all, major applications and/or general support systems as part of the disaster recovery exercise.

9.1.5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.10. Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

FY2013 Conclusion: Yes

Comments: N/A

9.1.11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.12. Contingency planning that consider supply chain threats. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

FY2013 Conclusion: 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 a public cloud. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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 (NIST SP 800-53: CA-2). (Base)

FY2013 Conclusion: Yes

Comments: We noted that while SSA management assessed the system security plan and planned for an independent assessment of controls for a contractor system, the assessment had not been executed prior to operation of the system.

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 a public cloud. (Base)

FY2013 Conclusion: Yes

Comments: We noted that the SSA contractor systems inventory did not include a service operated by a vendor. We noted that SSA had obtained a security controls assessment of this service.

10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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: N/A

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 11.1.2. Includes information security requirements as part of the capital planning and investment process. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 11.1.5. Ensures that information security resources are available for expenditure as planned. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

- 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.**

Comments: N/A

Appendix C – THE SOCIAL SECURITY ADMINISTRATION’S GENERAL SUPPORT SYSTEMS AND MAJOR APPLICATIONS

	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
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

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.

Appendix D – METRICS DEFINED

- **Continuous Monitoring Management** - Continuous Monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
- **Configuration Management** - 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.
- **Identify and Access Management** - Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files.
- **Incident Response and Reporting** - According to the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage.
- **Risk Management** – “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.*
- **Security Training** - According to FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002) an agency wide information security program for a Federal agency must include security awareness training. This training must cover (1) information security risks associated with users’ activities and (2) users’ responsibilities in complying with agency policies and procedures designed to reduce these risks.
- **Plan of Action and Milestones (POA&M)** – According to OMB M-14-04, “Plan of Action and Milestone (POA&M) (defined in OMB Memorandum M-02-01), A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.”
- **Remote Access Management** - Refers to controls associated with remote access to the information systems from virtually any remote location.

- **Contingency Planning** - Processes and controls to mitigate risks associated with interruptions (losing capacity to process, retrieve, and protect electronically maintained information) that may result in lost or incorrectly processed data.
- **Contractor Systems** - 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.
- **Security Capital Planning** – According to OMB M-14-04, “Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(C)) A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.”

Appendix E – MAJOR CONTRIBUTORS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Electronic Data Processing Partner, Grant Thornton

Cal Bassford, Director, Grant Thornton

Jessica Saunders, Senior Associate, Grant Thornton

Olga Mason, Senior Associate, Grant Thornton

Kevin Potter, Associate, Grant Thornton

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (<http://oig.ssa.gov/>) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "[Beyond The Numbers](#)" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.



[Watch us on YouTube](#)



[Like us on Facebook](#)



[Follow us on Twitter](#)



[Subscribe to our RSS feeds or email updates](#)

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at <http://oig.ssa.gov/audits-and-investigations/audit-reports/all>. For notification of newly released reports, sign up for e-updates at <http://oig.ssa.gov/e-updates>.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website: <http://oig.ssa.gov/report-fraud-waste-or-abuse>

Mail: Social Security Fraud Hotline
P.O. Box 17785
Baltimore, Maryland 21235

FAX: 410-597-0118

Telephone: 1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time

TTY: 1-866-501-2101 for the deaf or hard of hearing

OIG

Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's
Compliance with the Federal
Information Security Management
Act of 2002 for Fiscal Year 2013

A-14-13-13086 | November 2013

MEMORANDUM

Date: November 26, 2013

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 2013 (A-14-13-13086)

The attached final report summarizes Grant Thornton, LLP's, (Grant Thornton) Fiscal Year (FY) 2013 audit of the Social Security Administration's (SSA) information security program and practices, as required by Title III of the *E-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 we, or an independent external auditor, as determined by the Inspector General (IG), perform an annual evaluation that includes

- testing the effectiveness of SSA's information security policies, procedures, and practices of a representative subset of the agency's information systems and
- assessing compliance with FISMA requirements, and related information security policies, procedures, standards, and guidelines.

Under a contract we monitored, Grant Thornton, an independent certified public accounting firm, audited SSA's compliance with FISMA for FY 2013. Grant Thornton's report, along with its responses to the FY 2013 IG FISMA reporting metrics developed by the Department of Homeland Security (DHS), are submitted through CyberScope pursuant to Office of Management and Budget (OMB) Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*.

Objective, Scope, and Methodology

The objective of Grant Thornton's audit was to determine whether SSA's overall information security program and practices were effective and consistent with the FISMA requirements, as defined by DHS. In addition to FISMA and DHS' guidance, Grant Thornton tested SSA's overall information security program and practices using guidance from OMB and the National Institute of Standards and Technology, as well as SSA policy.

Grant Thornton conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Grant Thornton plan and perform

the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives.

Audit Results

For FY 2013, Grant Thornton determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. However, weaknesses identified limited the overall program's effectiveness in adequately protecting the Agency's information and information systems. Grant Thornton concluded that each of the metrics was generally consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology standards; however, Grant Thornton identified weaknesses in the following metrics:

Continuous Monitoring Management	Configuration Management	Identity and Access Management	Incident Response and Reporting	Risk Management
Security Training	Plan of Action & Milestones	Remote Access Management	Contingency Planning	Contractor Systems Oversight

Weaknesses in Sections 2, *Configuration Management* and 3, *Identity and Access Management*, resulted in negative conclusions to components of these metrics. For FY 2013, Grant Thornton concluded that the risk and severity of SSA's information security weaknesses were great enough to constitute a **significant deficiency** under FISMA.

OIG Evaluation of Grant Thornton's Audit Performance

To fulfill our responsibilities under the *Inspector General Act of 1978*, we monitored Grant Thornton's audit of SSA's FY 2013 compliance with FISMA by

- reviewing Grant Thornton's audit approach and planning;
- evaluating its auditors qualifications and independence;
- monitoring the audit progress;
- examining Grant Thornton's work papers;
- reviewing Grant Thornton's audit report to ensure compliance with Government Auditing Standards;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

Page 3 – The Commissioner

Grant Thornton is responsible for the attached auditor's report and the work and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton's performance under the terms of the contract. Our monitoring review, as described above, disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

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.

A handwritten signature in black ink, appearing to read "Pat O'Carroll Jr.", written in a cursive style.

Patrick P. O'Carroll, Jr.

Attachment



MEMORANDUM

Date: November 26, 2013
To: SSA Office of the Inspector General
From: Grant Thornton, LLP
Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013 (A-14-13-13086)

In conjunction with the audit of the Social Security Administration's (SSA) Fiscal Year (FY) 2013 Financial Statements, the Office of the Inspector General engaged us to conduct the performance audit on SSA's compliance with *Federal Information Security Management Act of 2002* (FISMA) for FY 2013. The objective was to determine whether SSA's overall information security program and practices were effective and consistent with the requirements of the FISMA as defined by the Department of Homeland Security. We are pleased to report the results of our audit and appreciate the support provided to us in completing this review.

Our report is intended solely for the information and use of management at SSA, SSA's Office of the Inspector General, the Office of Management and Budget, the Government Accountability Office, and Congress and is not intended to be and should not be used by anyone other than these specified parties.

Grant Thornton LLP

Alexandria, Virginia
November 26, 2013

The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013

November 2013

Report Summary

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

SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year 2013 FISMA performance audit in accordance with *Government Auditing Standards* commonly referred to as the "Yellow Book" which sets forth generally accepted government auditing standards. We assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and through performance of additional testing procedures as needed. We determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and other applicable regulations, standards, and guidance applicable during the audit period.

Our Findings

We determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. 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. We concluded that these weaknesses constituted a significant deficiency under FISMA.

Our Recommendations

- Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze current access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.
- Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.
- Address weaknesses identified within the comments of Appendix B by implementing our recommendations provided throughout the audit in our Notices of Finding and Recommendation.

TABLE OF CONTENTS

Objective	1
Background	1
Scope and Methodology	1
Results of Review	2
Agency Efforts to Resolve Weaknesses and Potential Cause for the FY 2013 FISMA Significant Deficiency	7
Conclusions and Recommendations	7
Views of Responsible Officials	8
Appendix A – Scope and Methodology	A-1
Appendix B – Response to Fiscal Year 2013 Inspector General <i>Federal Information Security Management Act</i> Reporting Metrics	B-1
Appendix C – The Social Security Administration’s General Support Systems and Major Applications	C-1
Appendix D – Metrics Defined	D-1
Appendix E – Major Contributors.....	E-1

ABBREVIATIONS

DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards Publication
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act of 2002
FSA	Financial Statement Audit
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAS	Government Auditing Standards
Grant Thornton	Grant Thornton LLP
IG	Inspector General
IT	Information Technology
NFR	Notice of Finding and Recommendation
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
PII	Personally Identifiable Information
Pub. L. No.	Public Law Number
SSA	Social Security Administration
U.S.C.	United States Code

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).

To achieve this objective, we assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems. We then determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and other regulations, standards, and guidance applicable during the audit period.

BACKGROUND

In conjunction with the audit of SSA's Fiscal Year (FY) 2013 Financial Statements,¹ SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the FY 2013 FISMA performance audit. FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002), includes the following key requirements:

- Each agency must develop, document, and implement an agency-wide information security program.²
- 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.³
- The agency's Inspector General (IG), or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.⁴

SCOPE AND METHODOLOGY

On November 30, 2012, DHS issued reporting metrics for the IG's FY 2013 FISMA submission. We audited the following 11 reporting metrics as part of our review:

¹ Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009.

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

³ Pub. L. No. 107-347, Title III, Section 301 § 3544(a)(1)(A); 44 U.S.C. § 3544(a)(1)(A).

⁴ 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).

FY 2013 Inspector General FISMA Reporting Metrics

- Continuous Monitoring Management
- Configuration Management
- Identity and Access Management
- Incident Response and Reporting
- Risk Management
- Security Training
- Plan of Action & Milestones (POA&M)
- Remote Access Management
- Contingency Planning
- Contractor Systems
- Security Capital Planning

The FY 2013 SSA FISMA performance audit was performed in accordance with *Government Auditing Standards* (GAS), issued by the Comptroller General of the United States, also known as the “Yellow Book” which sets forth generally accepted government auditing standards (GAGAS). We followed the Federal Information System Controls Audit Manual (FISCAM), which provides guidance for evaluating Electronic Data Processing general, and application controls in a Federal audit under GAGAS. In accordance with standards contained in GAS issued by the Comptroller General of the United States, we leveraged work performed as part of the FY 2013 Financial Statement Audit (FSA) and performed additional procedures as required to assess the reporting metrics listed above.

This report informs Congress and the public about SSA’s security performance and fulfills the Office of Management and Budget (OMB) and DHS requirements under FISMA to submit an annual report to Congress. Refer to Appendix A for additional information on our scope and methodology.

RESULTS OF REVIEW

For FY 2013, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements.⁵ However, weaknesses identified limited the overall program’s effectiveness to adequately protect the Agency’s information and information systems. We concluded that each of the metrics was generally

⁵ Our conclusion was based on our assessment of SSA’s compliance with DHS’ *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. 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 various issues in our assessment that are documented in the comments within Appendix B.

consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology (NIST) standards; however, we identified weaknesses in the following metrics:

Continuous Monitoring Management	Configuration Management	Identity and Access Management	Incident Response and Reporting	Risk Management
Security Training	POA&M	Remote Access Management	Contingency Planning	Contractor Systems Oversight

Refer to Appendix D for additional information on metrics.

Weaknesses in Section 2, *Configuration Management* and Section 3, *Identity and Access Management*, resulted in negative conclusions to the following metrics:

Configuration Management

- 2.1.4 – Process for timely (as specified in organization policy or standards) remediation of scan result deviations.
- 2.1.5 - For Windows-based components, United States Government Configuration Baselines (USGCB) secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented.
- 2.1.8 - Software assessing (scanning) capabilities are fully implemented.
- 2.1.9 - Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards.

Identity and Access Management

- 3.1.7 – Ensures that the users are granted access based on needs and separation-of-duties principles.
- 3.1.10 – Ensures that accounts are terminated or deactivated once access is no longer required.

We provided comments on these key components of SSA's information security program to Management throughout the audit.⁶ Refer to Appendix B for additional information on these and other weaknesses and conclusions.

We assessed the significance of these weaknesses individually and in the aggregate to determine the risk to SSA's overall information systems security program and management's control structure. We noted that while all these findings, in aggregate, impacted risk, the following weaknesses had the most significant impact on our conclusion:

- *Lack of a comprehensive Agency-wide policy and procedures related to vulnerability management, including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure/validation* - During internal penetration testing, we were able to take advantage of software vulnerabilities, misconfigurations, and restricted information to assume control of two servers, the Windows domain, as well as, gaining access to the mainframe without detection. This is the third successive year we have gained control of the SSA Windows system without detection. During subsequent assessments of the Agency's overall vulnerability management process, we noted that a key scanning tool was not being fully used to identify vulnerabilities across SSA's network, and Agency-wide comprehensive policies and procedures on vulnerability management were not established.

The Agency corrected the specific software vulnerabilities identified during our penetration testing, developed configuration standards for the software, and began using more capabilities of the scanning tool. However, without a comprehensive process in place, security threats may not be appropriately prioritized and remediated.

- *Lack of comprehensive Agency-wide policy and procedures related to management of application and system software changes, including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results* – While our testing demonstrated that change management activities were occurring for application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of the change management processes conducted by the Agency. Our testing noted the following.
 - System Software - An impact/risk assessment to determine the security implications for mainframe changes did not occur. Further, for the majority of changes tested, we noted that developers were responsible for testing their own changes and implementing these changes into production. While management performed a review to validate that updates made were associated with an approved change, there were no requirements nor guidance related to the types of testing to be performed (including security reviews), nor for retention or

⁶ We provided Agency management with a Notice of Finding and Recommendation (NFR) for each individual weakness. The NFR included the condition, criteria, cause, effect, and recommendation.

independent review of testing documentation, nor validation that the change made was limited to the requirements in the approved change ticket.

- Application Changes - We noted instances where evidence to support testing and other requirements could not be provided.

These issues increase the risk that changes to applications and supporting system software, which may impact benefit claim processing, payments, or financial data, do not function as intended or introduce security risks.

- *Lack of controls related to the identification and monitoring of high-risk programs operating on the mainframe⁷* - The Agency had not finalized and fully implemented controls associated with ensuring that privileged programs had been approved, could only be modified appropriately, and posed no security risks. Management continues making control enhancements including, but not limited to, identifying privileged programs, the review of privileged programs from a security perspective, access restrictions to all privileged programs, and change/monitoring control enhancements.

Without appropriate controls, there is an increased risk that the security posture and controls may be bypassed or compromised.

- *Access control issues* - Our testing identified numerous issues with logical access controls that are in place to mitigate the risk of unauthorized access. Our testing identified the following issues:
 - Access Authorization - Our testing identified control failures related to the appropriate completion of authorization forms. Included in these control failures were new hires, transferred employees, and contractors.
 - Access Removal - Our testing identified control failures related to the timely removal of terminated employees' logical access to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA and State Disability Determination Services employees who retained access after they were terminated. Additionally, SSA did not have an authoritative source to identify and manage all contractors and therefore SSA was unable to supply actual departure dates for contractors to substantiate timely removal of access.

⁷ 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.

- Profile⁸ Content and Analysis Review Program and Supporting Profile Controls - SSA Management continues to make progress in assessing profile content to validate that profiles only provide access to the minimal resources required for users to complete job functions. However, SSA had not completed the review of all profiles that are relevant to critical applications and supporting systems nor had SSA completed other profile quality initiatives including, but not limited to, some control enhancements.

As a result of these deficiencies, we noted numerous issues of unauthorized and inappropriate access including application developers (programmers) with unmonitored access to production data and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

For FY 2013, we concluded that the risk and severity of SSA's information security weaknesses, including those highlighted above and other weaknesses outlined in Appendix B, 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.⁹

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.”¹⁰

These security deficiencies, when aggregated, created a weakness in SSA's overall information systems security program that we concluded significantly compromised the security of its information and information systems.

⁸ 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.

⁹ **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).

¹⁰ OMB, M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013, page 8.

Agency Efforts to Resolve Weaknesses and Potential Cause for the FY 2013 FISMA Significant Deficiency

In response to the FY 2012 material weakness in information systems controls reported within the internal controls opinion¹¹ and FY 2012 FISMA significant deficiency,¹² SSA developed functional remediation teams to investigate issues, identify root causes, and implement corrective actions. Each functional remediation team, with oversight from SSA leadership, took risk-based approaches to remediation—addressing higher risk areas immediately, and planning for future security enhancements. Management’s risk based approach included correction of vulnerabilities identified through our specific tests as well as development and implementation of institutionalized and repeatable processes to prevent future weaknesses.

While SSA made significant efforts to strengthen controls over its systems and address weaknesses, our FY 2013 testing continued to identify general control issues in both design and operation of key controls. We believe that in many cases these deficiencies continue to exist because of one or a combination of the following:

- Control enhancements and newly designed controls require additional time to effectuate throughout the environment;
- By focusing resources on higher risk weaknesses, SSA was unable to implement corrective action for all aspects of the prior year issues; and/or,
- The design and/or operational effectiveness of enhanced or newly designed controls did not completely address risks.

SSA continues to implement corrective actions to address remaining deficiencies, which in many cases, is a continuation of previously established risk based strategies.

CONCLUSIONS AND RECOMMENDATIONS

For FY 2013, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. 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. We noted weaknesses within Section 2, *Configuration Management*, and Section 3, *Identity and Access Management*, that resulted in negative answers to metrics and various other issues that resulted in comments to the FISMA metrics located in Appendix B. Based on these factors, we concluded that these weaknesses constituted a significant deficiency under FISMA.

¹¹ Grant Thornton, *Independent Auditor’s Report* on the audit of SSA’s FY 2012 financial statements, November 8, 2012.

¹² SSA OIG, *The Social Security Administration’s Compliance with the Federal Information Security Management Act of 2002 for the Fiscal year 2012*, (A-14-12-12120), November 15, 2012.

SSA needs to 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.

To mitigate the risks of the issues noted in the significant deficiency, management should consider the following:

- Formally document comprehensive policies and procedures related to (1) threat identification and vulnerability management and (2) application and system software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze current access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and monitoring.
- Continue, as part of the SSA profile quality program, additional profile content reviews and other key profile improvement initiatives.
- Address weaknesses identified within the comments of Appendix B by implementing our recommendations provided throughout the audit in our Notices of Finding and Recommendation.

VIEWS OF RESPONSIBLE OFFICIALS

Our conclusions were discussed with SSA responsible officials who generally agreed with our findings and recommendations. SSA's official responses will be included in their comments to the independent auditor's report on the audit of SSA's FY 2013 financial statements.¹³

¹³ Grant Thornton, *Independent Auditor's Report* on SSA's FY 2013 financial statements will be released in December 2013.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency’s Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency’s information security programs and practices, as well as a review of an appropriate subset of agency systems.¹ The Social Security Administration’s (SSA) IG contracted with us, Grant Thornton LLP (Grant Thornton), to audit the SSA’s Fiscal Year (FY) 2013 financial statements.² Because of the extensive internal control system work that is completed as part of that audit, the FISMA review requirements were incorporated into our financial statement audit (FSA) contract. To maximize efficiencies and minimize the impact to SSA management during the FISMA performance audit, we used Appendix IX – *Application of FISCAM to FISMA* from the GAO *Federal Information System Controls Audit Manual* (FISCAM) in order to leverage testing performed during the SSA FSA. Additionally, governed by the 2011 *Government Audit Standards* Chapters 1 through 3, 6, and 7 – in particular Chapter 6, *Field Work Standards for Performance Audits - Using the Work of Others*, we leveraged the information technology general controls testing performed during the FSA wherever it was deemed appropriate. In some cases, FISMA tests were unique from those of the FSA; therefore, we designed test procedures to deliver adequate coverage over those unique areas.

Testing was performed in accordance with specific criteria as promulgated by the following:

- FISMA law;
- Office of Management and Budget (OMB) guidance;
- Department of Homeland Security (DHS) annual FISMA reporting instructions and annual FISMA IG reporting metrics, OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources;
- Standards and guidelines issued by the National Institute of Standards and Technology (NIST) – including, NIST Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*;
- Federal Information Processing Standards Publication (FIPS) - 199, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS-200 *Minimum Security Requirements for Federal Information and Information Systems*, FIPS- 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*;

¹ Pub. L. No. 107-347, Title III, Section 301 §§ 3545(a)(1), (a)(2)(A), (a)(2)(B); and (b)(1), 44 U.S.C. §§ 3545(a)(1) (a)(2)(A), (a)(2)(B); and (b)(1).

² Office of the Inspector General Contract Number GS-23F-8196H, December 3, 2009.

- Federal Information Security Memorandum 13-01, *FY 2013 Metrics for the Federal Information Security Management Act and Agency Privacy Management Act and Operational Reporting Instructions*;
- Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics; and,
- Local SSA policies.

Our assessment followed the DHS FY 2013 FISMA guidance³ 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 conducted this audit in accordance with generally accepted government auditing standards. These standards required 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 the audit objectives.

³ DHS Federal Information Security Memorandum 13-01, *FY 2013 Metrics for the Federal Information Security Management Act and Agency Privacy Management Act and Operational Reporting Instructions*, September 2013.

Appendix B – RESPONSE TO FISCAL YEAR 2013 INSPECTOR GENERAL *FEDERAL INFORMATION SECURITY MANAGEMENT ACT* REPORTING METRICS

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 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 SP 800-53, 800-53A). (AP)**

FY2013 Conclusion: Yes

Comments: We noted that the SSA continuous monitoring strategy includes manual control assessments and automated reporting mechanisms. Per the strategy, security controls currently selected for automated continuous monitoring are primarily technical controls that automated support tools can monitor and controls that may change frequently due to architectural or environment modifications such as updates and upgrades to hardware or software configurations. In regards to configuration standards, we noted that SSA made significant progress in developing baselines for authorized platforms in FY 2013; however, had not developed configuration baselines for all authorized platforms. In regards to vulnerability scanning capabilities, we noted the scanning tool used

by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

- 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 a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). (AP)**

FY2013 Conclusion: Yes

Comments: We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per the continuous monitoring strategy, the successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

- 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: N/A

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?**

FY2013 Conclusion: Yes

- 2.1.1. Documented policies and procedures for configuration management. (Base)**

FY2013 Conclusion: Yes

Comments: We noted that while compartmentalized policies and procedures existed, SSA lacked a comprehensive Agency-wide policy and procedures related to application and system software change management including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results.

- 2.1.2. Defined standard baseline configurations. (Base)**

FY2013 Conclusion: Yes

Comments: We noted that SSA established a list of authorized infrastructure software (platforms), had developed baselines for the majority of key platforms, and made significant progress in developing additional configuration baselines in FY 2013. However, it had not developed configuration baselines for all authorized platforms. Further, requirements associated with approval to deviate from agency security standards or configurations by submitting an exception request for software not on the authorized platform list were not in place during the entire fiscal year.

2.1.3. Assessments of compliance with baseline configurations. (Base)

FY2013 Conclusion: Yes

Comments: We noted the following regarding compliance with baseline configurations:

- Lack of configuration baselines for some platforms;
- Internal penetration testing identified high risk vulnerabilities due to unpatched software and misconfigurations, which resulted in testers obtaining domain administrative rights and access to the mainframe; and,
- Assessments of key configurations and access rights on significant platforms identified issues including misconfigurations.

2.1.4. Process for timely (as specified in organization policy or standards) remediation of scan result deviations. (Base)

FY2013 Conclusion: No

Comments: We noted that SSA had processes in place for remediation of results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

2.1.5. For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. (Base)

FY2013 Conclusion: No

Comments: We noted that documentation for a significant number of deviations from the USGCB settings did not provide sufficient information pertaining to risk analysis and business justification for the deviation.

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

FY2013 Conclusion: Yes

Comments: We noted that while testing demonstrated that change management activities were occurring for both application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of change management processes conducted by the Agency. In addition, our testing identified system software weaknesses including completion of impact risk assessments, completion of test plans and retention of testing output, independent review of testing as well as validation changes were limited to those identified in the change request. For application changes, we noted instances where evidence to support testing and other requirements could not be provided.

In addition, the Agency had not finalized and fully implemented controls associated with ensuring that mainframe privileged programs have been approved, can only be modified appropriately, and pose no security risks.

2.1.7. Process for timely and secure installation of software patches. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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

FY2013 Conclusion: No

Comments: We noted the scanning tool used by the Security Operations Center was not being utilized to its full capability for part of the fiscal year.

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

FY2013 Conclusion: No

Comments: We noted that SSA had processes in place for remediation of scan results identified through scanning and internal penetration testing. However, we noted SSA lacked a comprehensive Agency-wide policy and procedures related to vulnerability management including security vulnerability identification, prioritization, categorization, remediation, tracking, and closure / validation. Without appropriate prioritization, higher risk vulnerabilities may not be

remediated timely as demonstrated by internal penetration testing results. In addition, misconfigurations were identified through testing of configurations on key platforms.

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

FY2013 Conclusion: Yes

Comments: We noted that SSA had established a patch management process; however, issues associated with the ability to identify and remediate vulnerabilities in a timely manner impact the Agency's ability to prioritize software patches. Without appropriate prioritization, higher risk vulnerabilities may not be remediated timely as demonstrated by internal penetration testing results.

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: N/A

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 which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). (Base)

FY2013 Conclusion: Yes

Comments: Although the Agency was able to identify all users, including contractors, with access to the mainframe and all employees with access to the

network, SSA did not have an authoritative source / system(s) that identified and managed all contractors.

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

FY2013 Conclusion: Yes

Comments: We noted that SSA identified when special access requirements were necessary; however, we also noted that application developers had access to the production environment. These users did not obtain this access through the secondary ID process, which is a highly monitored process whereby programmers gain access to production for a limited time, and activity is subject to review.

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

FY2013 Conclusion: Yes

Comments: N/A

3.1.5. Organization has 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). (AP)

FY2013 Conclusion: Yes

Comments: N/A

3.1.6. Organization has adequately planned for implementation of PIV for physical 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).

FY2013 Conclusion: Yes

Comments: N/A

3.1.7. Ensures that the users are granted access based on needs and separation-of-duties principles. (Base)

FY2013 Conclusion: No

Comments: We identified numerous issues with logical access controls which resulted in inappropriate and / or unauthorized access including application developers (programmers) with unmonitored access to production and application transactions, access to key transactions and data, key change management libraries, and other sensitive system software resources.

3.1.8. 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.) (Base)

FY2013 Conclusion: Yes

Comments: The OIG Audit Report A-14-13-13050, *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network*, noted that while the Agency has a process to identify hardware devices connected to its network, we [the IG] determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA has processes to monitor the security level of connected devices, they were inconsistent with Agency policy in effect at the time of our [the IG] audit.

3.1.9. Identifies all user and non-user accounts (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users) (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA was able to identify user and non-user accounts. However, we noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

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

FY2013 Conclusion: No

Comments: We identified control failures related to the timely removal of logical access for terminated employees to the mainframe, network, and other supporting systems. Included in these control failures were instances of SSA employees and state Disability Determination Services employees. Additionally, SSA did not have an authoritative source that identified and managed all contractors and therefore was unable to support actual departure dates for contractors.

3.1.11. Identifies and controls use of shared accounts. (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where default account passwords had not been changed, access to a generic account that was not required by a user, a lack of

requirements to periodically change passwords for system accounts, and issues associated with the management of vendor accounts.

- 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: N/A

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 4.1.2. Comprehensive analysis, validation and documentation of incidents. (KFM)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 4.1.4. When applicable, reports to law enforcement within established timeframes (SP 800-61). (KFM)**

FY2013 Conclusion: Yes

Comments: We noted the incident reporting policy included information about reporting of incidents to law enforcement including but not limited to the OIG, Federal Protective Services and local law enforcement; however, the policy did

not specify the established timeframes in which incidents should be reported to law enforcement.

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

FY2013 Conclusion: Yes

Comments: We noted that the SSA incident response procedures did not provide guidance or directives associated with establishing timeframes in which incidents should be resolved.

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

FY2013 Conclusion: Yes

Comments: N/A

4.1.7. Is capable of correlating incidents. (Base)

FY2013 Conclusion: Yes

Comments: N/A

4.1.8. Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA had a comprehensive governance structure and organization-wide risk management strategy. However, we noted instances where off-site locations did not consistently apply SSA guidance such as requirements within the Program Operations Manual System.

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.5. Has an up-to-date system inventory. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.6. Categorizes information systems in accordance with government policies. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.7. Selects an appropriately tailored set of baseline security controls. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.9. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.10. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.11. 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. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA continued to enhance automated continuous monitoring reporting capabilities in FY 2013. Per SSA's continuous monitoring strategy, successful implementation of the SSA continuous monitoring strategy will require a sustained effort contingent upon the availability of funding and support from Agency components.

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.13. Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). (Base)

FY2013 Conclusion: Yes

Comments: N/A

5.1.14. 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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

5.1.16. Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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: N/A

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?

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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. (KFM)

FY2013 Conclusion: Yes

Comments: We noted that SSA did not have an authoritative source / system(s) that identified and managed all contractors. Therefore, we were not able to gain reasonable assurance that the contractor population was complete. Without a complete population, the Agency may not be able to identify and track all contractors that require security awareness training. In addition, we noted that security training was not completed in a timely fashion for all employees and contractors (those that we were able to assess) or evidence to support completion of security training was not provided.

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. (KFM)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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?

FY2013 Conclusion: Yes

7.1.1. Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. (Base)

FY2013 Conclusion: Yes

Comments: We noted that although key activities associated with tracking and monitoring IT security weaknesses were being performed, Management had not fully documented a comprehensive policy and procedures covering all of the Agency's processes. Current policies and procedures associated with tracking of IT weaknesses, including the POA&M process, did not encompass the multiple tools and methods used by Management.

7.1.2. Tracks, prioritizes and remediates weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where Information Technology security weaknesses were inadvertently "closed" within the Agency's tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

7.1.3. Ensures remediation plans are effective for correcting weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.4. Establishes and adheres to milestone remediation dates. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.5. Ensures resources and ownership are provided for correcting weaknesses. (Base)

FY2013 Conclusion: Yes

Comments: N/A

7.1.6. POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)

FY2013 Conclusion: Yes

Comments: We noted instances where Information Technology (IT) security weaknesses were inadvertently “closed” within the Agency’s tracking tool even though they remained open. It was noted that these items were subsequently corrected by Management.

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

FY2013 Conclusion: Yes

Comments: N/A

7.1.8. Program officials 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; OMB M-04-25). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 8.1.2. Protects against unauthorized connections or subversion of authorized connections. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 8.1.4. Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)**

FY2013 Conclusion: Yes

Comments: We noted that SSA's revised telework policy was in draft form pending resolution of administrative matters.

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

FY2013 Conclusion: Yes

Comments: N/A

8.1.6. Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

8.1.8. Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: N/A

8.3. Does the organization have a policy to detect and remove unauthorized (rogue) connections?

FY 2013 Conclusion: Yes

Comments: 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?

FY2013 Conclusion: 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 SP 800-53: CP-1). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.2. The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

9.1.4. Testing of system specific contingency plans. (Base)

FY2013 Conclusion: Yes

Comments: We noted that SSA tested the majority of, but not all, major applications and/or general support systems as part of the disaster recovery exercise.

9.1.5. The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.6. Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.7. Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.8. After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.9. Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.10. Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).

FY2013 Conclusion: Yes

Comments: N/A

9.1.11. Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY2013 Conclusion: Yes

Comments: N/A

9.1.12. Contingency planning that consider supply chain threats. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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.

Comments: 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? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

FY2013 Conclusion: 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 a public cloud. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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 (NIST SP 800-53: CA-2). (Base)

FY2013 Conclusion: Yes

Comments: We noted that while SSA management assessed the system security plan and planned for an independent assessment of controls for a contractor system, the assessment had not been executed prior to operation of the system.

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 a public cloud. (Base)

FY2013 Conclusion: Yes

Comments: We noted that the SSA contractor systems inventory did not include a service operated by a vendor. We noted that SSA had obtained a security controls assessment of this service.

10.1.4. The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). (Base)

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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: N/A

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?**

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

- 11.1.2. Includes information security requirements as part of the capital planning and investment process. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

- 11.1.5. Ensures that information security resources are available for expenditure as planned. (Base)**

FY2013 Conclusion: Yes

Comments: N/A

- 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.**

Comments: N/A

Appendix C – THE SOCIAL SECURITY ADMINISTRATION’S GENERAL SUPPORT SYSTEMS AND MAJOR APPLICATIONS

	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
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

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.

Appendix D – METRICS DEFINED

- **Continuous Monitoring Management** - Continuous Monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
- **Configuration Management** - 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.
- **Identify and Access Management** - Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files.
- **Incident Response and Reporting** - According to the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage.
- **Risk Management** – “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.*
- **Security Training** - According to FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002) an agency wide information security program for a Federal agency must include security awareness training. This training must cover (1) information security risks associated with users’ activities and (2) users’ responsibilities in complying with agency policies and procedures designed to reduce these risks.
- **Plan of Action and Milestones (POA&M)** – According to OMB M-14-04, “Plan of Action and Milestone (POA&M) (defined in OMB Memorandum M-02-01), A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.”
- **Remote Access Management** - Refers to controls associated with remote access to the information systems from virtually any remote location.

- **Contingency Planning** - Processes and controls to mitigate risks associated with interruptions (losing capacity to process, retrieve, and protect electronically maintained information) that may result in lost or incorrectly processed data.
- **Contractor Systems** - 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.
- **Security Capital Planning** – According to OMB M-14-04, “Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(C)) A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.”

Appendix E – MAJOR CONTRIBUTORS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Electronic Data Processing Partner, Grant Thornton

Cal Bassford, Director, Grant Thornton

Jessica Saunders, Senior Associate, Grant Thornton

Olga Mason, Senior Associate, Grant Thornton

Kevin Potter, Associate, Grant Thornton

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (<http://oig.ssa.gov/>) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "[Beyond The Numbers](#)" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.



[Watch us on YouTube](#)



[Like us on Facebook](#)



[Follow us on Twitter](#)



[Subscribe to our RSS feeds or email updates](#)

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at <http://oig.ssa.gov/audits-and-investigations/audit-reports/all>. For notification of newly released reports, sign up for e-updates at <http://oig.ssa.gov/e-updates>.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website: <http://oig.ssa.gov/report-fraud-waste-or-abuse>

Mail: Social Security Fraud Hotline
P.O. Box 17785
Baltimore, Maryland 21235

FAX: 410-597-0118

Telephone: 1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time

TTY: 1-866-501-2101 for the deaf or hard of hearing