



SOCIAL SECURITY

The Commissioner

February 29, 2016

The Honorable Jason Chaffetz
Chairman, Committee on Oversight and
Government Reform
House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

We are pleased to provide you with our fiscal year 2015 Federal Information Security Modernization Act report as required by the Office of Management and Budget's Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. Our report includes our responses to the reporting questions as well as the reports of our Senior Agency Official for Privacy and our Office of the Inspector General (OIG). The OIG's report includes an independent evaluation of our information security program.

I hope you find the information helpful. Pursuant to the requirements of M-16-03, I am sending a transmittal letter with the report to the following House Committees: Oversight and Government Reform; Science, Space, and Technology; Homeland Security; Appropriations; and Ways and Means. I am also sending a transmittal letter with the report to the following Senate Committees: Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; Finance; and Appropriations.

If you have any questions, please have your staff contact Robert Klopp, our Chief Information Officer, at (410) 965-8399, or by email at Robert.Klopp@ssa.gov.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure



SOCIAL SECURITY

The Commissioner

February 29, 2016

The Honorable Ron Johnson
Chairman, Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

We are pleased to provide you with our fiscal year 2015 Federal Information Security Modernization Act report as required by the Office of Management and Budget's Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. Our report includes our responses to the reporting questions as well as the reports of our Senior Agency Official for Privacy and our Office of the Inspector General (OIG). The OIG's report includes an independent evaluation of our information security program.

I hope you find the information helpful. Pursuant to the requirements of M-16-03, I am sending a transmittal letter with the report to the following House Committees: Oversight and Government Reform; Science, Space, and Technology; Homeland Security; Appropriations; and Ways and Means. I am also sending a transmittal letter with the report to the following Senate Committees: Homeland Security and Governmental Affairs; Commerce, Science, and Transportation; Finance; and Appropriations.

If you have any questions, please have your staff contact Robert Klopp, our Chief Information Officer, at (410) 965-8399, or by email at Robert.Klopp@ssa.gov.

Sincerely,

Carolyn W. Colvin
Acting Commissioner

Enclosure



SOCIAL SECURITY

The Commissioner

November 27, 2015

The Honorable Shaun Donovan
Director, Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Donovan:

We are pleased to submit our fiscal year (FY) 2015 Information Technology Security Program Review Report, as required by the Federal Information Security Modernization 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). Our OIG's report includes an independent evaluation of our information security program and FISMA compliance.

In accordance with the Office of Management and Budget's (OMB) Memorandum M-16-03, "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," we offer the following assessment of the adequacy and effectiveness of our information security and privacy policies, procedures and practices in the following areas:

1. Progress towards meeting FY 2015 FISMA metrics;
2. Progress towards meeting the Cybersecurity Cross-Agency Priority (CAP) goals; and,
3. Information on Cybersecurity Incidents.

1. Progress towards meeting FY 2015 FISMA metrics

Our Grant Thornton financial statement auditors found that our progress toward meeting the FY 2015 FISMA metrics resulted in a high degree of compliance. We successfully met all metrics in the areas of Continuous Monitoring, Plans of Action and Milestones, Remote Access Management, Contingency Planning, and Contractor Systems. Our auditors also found that we have made significant progress in strengthening controls over our information systems to address the significant deficiency the auditors found last year. We are pleased that based upon our successful mitigation efforts the auditors removed mainframe security as one of the conditions of the significant deficiency. While we are aggressively pursuing several initiatives to strengthen our controls, some of the underlying causes require continued long-term commitment.

OIG Findings

In FY 2015, the auditor also noted that we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources. We improved our existing controls and implemented new controls and risk management processes, yet auditors reduced our overall score compared to the FY 2014 review. In the areas of Configuration Management, Identity and Access Management, Incident Response and Reporting, and Security Training, the auditor determined that we established an information security program and practices that were generally consistent with FISMA requirements and that we met the majority of metrics. However, in the area of Risk Management, the auditors cited some findings that they consider might limit our ability to adequately protect the organization's information and information systems.

We disagree with the reduced compliance scores cited by our auditor in the area of Risk Management. We completed action on many recommendations from the FY 2014 FISMA assessment, and continue to address open recommendations. We prioritized our actions for improvement to address the most significant risks first. For example, in FY 2015 we reduced the number of privileged accounts, increased the number of individuals who use Personal Identify Verification (PIV) cards, expanded our penetration-testing program to include external testing, added additional cyber hygiene scans, and published an agency wide change management directive.

The auditor indicated that Risk Management compliance decreased because there are an extensive number of applications hosted at decentralized locations. These findings extend to disability case processing systems, hosted at Disability Determination Services (DDS) locations. However, in FY 2015 we improved our controls on these decentralized applications. In the last quarter of FY 2015, we completed risk assessments for the distributed software applications specifically identified by Grant Thornton in FY 2014 and 2015. We determined that the risk associated with these applications as low because regional applications are smaller in scope and do not process programmatic or financial transactions. The regional applications do not access financial systems. Almost half of these "applications" are region-specific tools that do not contain personal information, e.g., spreadsheets or static SharePoint sites. Due to the lack of financial impact or significance, we consider these applications lower risk.

Regional Application Security Assessment

We broadened our mature and robust process for assessing the security of our mission-critical systems to include our regional applications. As part of a multi-year effort to extend our robust risk management protocols to all decentralized software applications, we developed a standardized Security Assessment and Authorization (SA&A) process to apply to regionally developed applications. We increased our staffing in the SA&A area to accelerate the roll out of the standard regional SA&A process. Our newly developed SA&A process for these regionally developed applications, includes assigning them security authorization boundaries, as well as documenting and assessing the security controls in place. By the first quarter of FY 2016, we plan to implement our new standard SA&A process to manage security risks for regionally developed applications in a comprehensive and consistent manner. While we did not fully implement our new SA&A process in FY 2015, we made significant progress, including the development of a complete and accurate inventory. Based on our improved oversight, we do not think there is justification for our increased risk management score in this area, rather than a decrease.

Disability Determination Services (DDS) Application Security Assessment

We standardized system security plans for DDS and continue to improve governance and oversight over DDS processes. We manage contracts to operate, change, and replace DDS systems. Our contract managers maintain oversight, control, and monitoring of these systems. We have security risk configuration standards and scans for the DDS systems. We continue to improve in this area, and in FY 2015, our compliance improved over 2014 with the implementation of the security plans and changes to disability security policies. Additionally in FY 2016, we will enhance governance over the DDS systems when we implement the Disability Case Processing System (DCPS). DCPS will provide standard system infrastructure for all DDS processes.

We employ a strong set of security controls, technologies, policies and procedures to manage risk. We continue to make ongoing improvements to our risk management protocols to keep pace with changes in the operating environment, mitigate known risks, and address prior audit recommendations. Throughout this audit, we engaged Grant Thornton to explain our approach, provide documentation of our progress, and obtain feedback on their assessment.

2. Progress towards meeting the Cybersecurity CAP goals

Our Performance Improvement Officer reviewed our progress towards meeting the nine Cybersecurity CAP goals for FY 2015. We met the following eight goals:

1. Anti-phishing Defense;
2. Malware Defense;
3. Blended Defense (Anti-Phishing and Malware defense measures);
4. Hardware Asset Management;
5. Software Asset Management;
6. Vulnerability and Weakness Management;
7. Security Configuration Management; and,
8. Personal Identity Verification (PIV) Unprivileged.

Regarding the 9th Cybersecurity CAP goal, we are at 99 percent for privileged users' usage of PIV credentials. While this is slightly under the Cybersecurity CAP goal of 100 percent, we are diligently working toward meeting this CAP goal through the procurement of a new solution and refinement of our existing processes.

3. Information on Cybersecurity Incidents

We had no occurrences of major computer security incidents as defined in OMB's Memorandum M-16-03 for FY 2015. We have reported 1033 cyber incidents through the Department of Homeland Security, Computer Emergency Readiness Team (US-CERT) incident notification system in FY 2015. This number does not include the paper incidents that we reported. Reported incidents occurred on the devices in our field offices, regional offices, hearing offices, data centers, and headquarters. Please refer to the charts below for type of incidents and impact levels.

Type of Cyber Incidents

Types of Incidents	Counts
Category 0 – Exercise	1
Category 1 – Unauthorized Access	65
Category 3 – Malicious Code	128
Category 4 – Improper Usage	303
Category 5 – Scans	4
Category 6 – Under Investigation by US-CERT	179
Category 6 – Under Investigation by SSA	2
Uncategorized By US-CERT	351
Total	1033

Cyber Incidents Impact Levels

Impact levels	Counts
Medium	38
Low	778
Minimum	11
None	206
Total	1033

Thank you for the opportunity to offer our assessment of the adequacy and effectiveness of our information security and privacy policies, procedures and practices. If I may be of further help, please contact me, or your staff may contact Robert Klopp, our Chief Information Officer, at (410) 965-8399 or by email at Robert.Klopp@ssa.gov.

Sincerely,



Carolyn W. Colvin
Acting Commissioner

Enclosure

Chief Information Officer

Section Report

2015
Annual FISMA
Report

Social Security Administration

Section 1A: System Inventory

- 1.1 For each FIPS 199 impact level, what is the total number of operational unclassified information systems by organization (i.e. Bureau or Sub-Department Operating Element) categorized at that level? (Organizations with fewer than 5,000 users may report as one unit.)
Answer in the table below.

		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 (signed, in scope)
SSA				
	High	0	0	0
	Moderate	15	0	15
	Low	5	0	5
	Not Categorized	0	0	0
	Sub-Total	20	0	20
Agency Totals				
	High	0	0	0
	Moderate	15	0	15
	Low	5	0	5
	Not Categorized	0	0	0
	Total	20	0	20

Section 1B: System Inventory

- 1.2 How many endpoints belong to systems without a valid ATO?

0

- 1.3 How many public facing systems are without a valid ATO?

0

Section 2A: ISCM - Hardware/Software Asset Management

Hardware Asset Management

- 2.1 What is the total number of the organization's hardware assets connected to the organization's unclassified network(s)?

315619

- 2.1.1 Percent (%) of assets from 2.1 that store (e.g., on an endpoint or maintained as a record in an external asset management database) meta-data (e.g. system association, owner, location)?
100%

- 2.1.2 What is the total number of endpoints connected to the organization's unclassified network(s)?

315619

Section 2A: ISCM - Hardware/Software Asset Management

2.2 Percent (%) of the organization's network fabric covered by a capability to detect and alert on the addition of unauthorized hardware assets onto the organization's network.

100%

2.3 Percent (%) of the organization's network fabric covered by an automatic capability (scans/device discovery processes) that provides enterprise-level visibility into the current state of all hardware assets.

100%

2.4 What is the mean time to detect a new device (time between scans in 2.2)?

0.0

Comments: zero days

2.5 Percent (%) of the organization's registered network fabric covered by a Network Access Control switching technology that blocks unauthorized devices.

7%

Comments:

SSA has deployed Network Access Control (NAC) solutions for internal wireless network and for remote network access. Endpoints are required to undergo a security posture assessment to ensure security compliance prior to granting endpoints network access into SSA's internal network. SSA is studying the feasibility of deploying a NAC solution for SSA's internal Ethernet network for CY 2018.

Software Asset Management

2.6 Percent (%) of endpoints from 2.1.2 covered by an automated software asset inventory capability to scan the current state of installed software (e.g., .bat, .exe, .dll).

100%

2.7 Percent (%) of endpoints from 2.1.2 covered by a desired-state software asset management capability to detect and block unauthorized software from executing (e.g., AppLocker, certificate, path, hash value, services, and behavior based whitelisting solutions).

100%

2.8 How many major application databases does the organization maintain?

127

Comments:

The answer of 127 reflects those databases associated to our agency's major applications. Our agency inventory of databases includes these major application databases plus additional databases.

2.9 Percent (%) of the organization's network fabric that undergoes periodic discovery scanning specifically for the purpose of identifying and enumerating databases.

Section 2A: ISCM - Hardware/Software Asset Management

100%

Comments:

A majority of our major application databases reside on mainframe-attached storage. We centrally manage these databases with mature change management controls to prevent unauthorized changes to production databases. We perform continuous, recurring network discovery scans on our network to identify and enumerate databases on the network.

Section 2B: ISCM - Secure Configuration Management

- 2.10 Please complete the table below. Future configurations will be added as needed. Data calls for layer 2, layer 3, mobile, printers, or other devices or operating systems will be used as needed.

Comments:

Columns 2.10.4 and 2.10.5 represent days.

List of top U.S. Government Operating Systems, as reported in SCAP feeds	2.10.1 What is the number of hardware assets with each OS?	2.10.2 What is the common security configuration baseline for each OS listed? (e.g., USGCB)	2.10.3 How many configuration exceptions are granted by the enterprise?	2.10.4 What is organization's enterprise policy for maximum audit interval (target)?	2.10.5 What is organization's enterprise average audit interval (actual)?	2.10.6 Percent (%) of assets in 2.10.1 covered by the auditing activities described in 2.10.4 and 2.10.5
Windows 8.x	5	Agency Provided	0	14.00	14.00	100%
Windows 7.x	161,805	Agency Provided	1	14.00	14.00	100%
Windows Vista	130	Agency Provided	0	14.00	14.00	100%
Windows Unsupported (include XP)	5					
Windows Server 2003	541	Agency Provided	2	14.00	14.00	100%
Windows Server 2008	5,001	Agency Provided	0	14.00	14.00	100%
Windows Server 2012	12,183	Agency Provided	0	14.00	14.00	100%
Linux (all versions)	233	Agency Provided	1	14.00	14.00	100%
Unix / Solaris (all versions)	801	Agency Provided	0	14.00	14.00	100%
Mac OS X	6	Agency Provided	1	14.00	14.00	100%

Section 2C: ISCM - Vulnerability and Weakness Management

- 2.11 Percent (%) of hardware assets listed in 2.1 assessed using credentialed scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.

100%

- 2.12 What is the mean time between vulnerability scans?

14.00

Section 2C: ISCM - Vulnerability and Weakness Management

Comments:

Days

2.13 Percent (%) of the databases in 2.8 that undergo periodic vulnerability scanning with a special purpose database vulnerability scanner.

5%

Comments:

The majority of our major application databases reside on mainframe-attached storage. We centrally manage and protect our mainframe production database with multiple layers of safeguards including privileged access and change management controls. We perform periodic vulnerability scans for Oracle databases on our distributed network

2.14 What is the mean time to mitigate for high findings?

14.00

Comments:

Days

Section 3: Identity Credential and Access Management

Unprivileged Network Users

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

89375

3.1.1 Percent (%) of users from 3.1 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential.

86%

Privileged Network Users

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

7153

3.2.1 Percent (%) of users from 3.2 technically required to log onto the network with a two-factor PIV card or NIST Level of Assurance (LOA) 4 credential.

99%

3.3 Percent (%) of privileged network users that had their privileges reviewed this year.

100%

3.4 Percent (%) of privileged network users that had their privileges adjusted or terminated after being reviewed this year.

23%

Section 3: Identity Credential and Access Management

Internal Systems

- 3.5 Percent (%) of the organization's internal systems configured to require PIV authentication.
1%
- 3.6 Percent (%) of the organization's government service portals (e.g., Max.gov Portal, MyEPP) that enforce PIV authentication for cross-agency federal customers. (If none are provided, answer N/A.)
N/A

Remote and Mobile Device Access Solutions

- 3.7 How many users log onto the organization's remote access solution(s) to obtain access to the organization's desktop LAN/WAN resources or services?
18292

3.7.1 Percent (%) of the users reported in 3.7 required to use two-factor PIV card authentication to remotely log onto the organization's desktop LAN/WAN resources or services
100%

- 3.8 How many users are enabled to remotely log onto the organization's LAN/WAN resources or services from mobile devices?
5739

Comments:

We do not allow remote access from mobile devices to our desktop LAN/WAN resources, with the exception of specific web-based services. We plan to implement a certificate-based authentication for all of our mobile devices.

3.8.1 Of the organization's users who remotely access desktop LAN/WAN resources or services from mobile devices, what percent (%) of these users are technically required to use two-factor PIV card authentication to access these resources and services?
0%

Comments:

We do not allow remote access from mobile devices to our desktop LAN/WAN resources.

Physical Access Control Systems

3.9 Percent (%) of agency's operational Physical Access Control Systems (PACS) that comply with procurement requirements for purchasing products and services from the FIPS 201 Approval Products List maintained by General Services Administration (GSA) (per OMB M06-18).
100%

3.10 Percent (%) of agency's operational PACS that electronically accept and authenticate internal users' PIV credentials for routine access in accordance with NIST standards and guidelines (e.g., FIPS 201-2 and NIST SP 800-116).

Section 3: Identity Credential and Access Management

100%

Section 4: Anti-Phishing and Malware Defense

4.1 Percent (%) of privileged user accounts that have a technical control preventing internet access.

0%

Comments:

SSA has the capability to prevent privileged users from accessing the Internet but this capability is not implemented.

4.2 Percent (%) of incoming email traffic analyzed for clickable URLs, embedded content, and attachments.

100%

Comments:

SSA actively removes malicious links, malicious embedded content and malicious attachments from incoming email.

4.3 Percent (%) of hardware assets covered by a host-based intrusion prevention system.

0%

Comments:

SSA uses network-based intrusion detection/prevention systems to protect against endpoint threats. However, SSA has not deployed host-based intrusion prevention systems to its endpoints.

4.4 Percent (%) of hardware assets covered by an antivirus (AV) solution using file reputation services, checking files against cloud-hosted, continuously updated malware information.

100%

Comments:

SSA deploys an antivirus (AV) solution to its endpoints that uses a signature-based subscription service.

4.5 Percent (%) of email attachments opened in sandboxed environment or detonation chamber.

0%

Comments:

We review all email attachments in real time for malicious content and all email attachments that contain such content is stripped and deleted. We are piloting use of a sandbox technology for screening email

4.6 Percent (%) of incoming emails using email sender authentication protocols such as DomainKeys Identified Mail (DKIM), Author Domain Signing Practices (ADSP), Domain-based Message Authentication, Reporting & Conformance (DMARC), Vouch by Reference (VBR), or IP Reverse (iprev).

100%

Comments:

SSA uses Sender Policy Framework (SPF) to validate the identity of email senders.

4.7 Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.

100%

Section 4: Anti-Phishing and Malware Defense

Comments:

For incoming email filtering, SSA uses a reputation filter tool for determining malicious senders.

4.8 **Percent (%) of hardware assets covered by an anti-exploitation tool (e.g., Microsoft's Enhanced Mitigation Experience Toolkit (EMET) or similar).**

0%

Comments:

SSA has not deployed Microsoft's EMET due to endpoint performance concerns discovered during testing.

4.9 **Percent (%) of inbound email traffic passing through anti-phishing/anti-spam filtration technology at the outermost border Mail Transport Agent or email server.**

100%

Comments:

SSA filters 100% of SSA's inbound email using an enterprise anti-phishing/anti-spam filtering solution with the filtering occurring at the outermost email server/mail transfer agent

4.10 **Percent (%) of inbound network traffic that passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites (e.g., fake software updates, fake antivirus offers, and phishing offers).**

100%

Comments:

SSA conducts inbound/outbound web content filtering at the proxy gateway. SSA's web content filtering protection includes protection against phishing, malware, and malicious sites.

4.11 **Percent (%) of hardware assets that have implemented a browser-based (e.g., Microsoft Phishing filter) or enterprise-based tool to block known phishing websites and IP addresses.**

100%

Comments:

SSA conducts anti-phishing filtering at the proxy gateway.

4.12 **Percent (%) of outbound communications traffic checked at the external boundaries to detect covert exfiltration of information.**

100%

Comments:

SSA uses a data loss prevention solution that actively protects the agency against the exfiltration of PII.

4.13 **Percent (%) of sent email that is digitally signed.**

100%

Comments:

We have the technical capability to sign email digitally; however, the end user performs digital signing manually.

4.14 **Percent (%) of email traffic quarantined or otherwise blocked.**

100%

Comments:

SSA has the technical capability to block and/or quarantine malicious email traffic but does not track the metric of these

Section 4: Anti-Phishing and Malware Defense

events regularly. SSA is in the process of implementing a regular scheduled solution to track and report these events.

Section 5: Data Protection

5.1 What is the estimated number of hardware assets in each of the following mobile and portable asset types, and how many are encrypted? Answer in the table below.

Mobile and Portable Device Types (each asset should be recorded no more than once in each column).	5.1.1 Estimated number of mobile hardware assets of the types indicated in each row.	5.1.2 Estimated number of assets from 5.1.1 with FIPS 140-2 compliant encryption of data on the device.
Laptop computers and netbooks	44664	100
Tablet-type computers	154	100
Smartphones	5739	100
Other mobile devices	0	0

Section 6: Network Defense

6.1 What is the estimated percent (%) of remote access connections that have each of the following properties:

- 6.1.1 Percent (%) that utilize FIPS 140-2-validated cryptographic modules.
100%
- 6.1.2 Percent (%) that prohibit split tunneling and/or dual-connected remote hosts where the mobile device has two active connections.
100%
- 6.1.3 Percent (%) configured in accordance with OMB M-07-16 to time-out after 30 minutes of inactivity (or less) and requires re-authentication to reestablish session.
100%
- 6.1.4 Percent (%) scanned for malware upon connection.
100%

Comments:

Before we permit access, we scan all hosts for the correct antivirus software version and antivirus signature. We quarantine incorrectly configured hosts.

Section 7: Boundary Protection

Instruction: Questions 7.1 – 7.3 do not apply to the Department of Defense.

7.1 Percent (%) of the required TIC 2.0 Capabilities implemented.

Section 7: Boundary Protection

98%

Questions 7.2–7.3 apply only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.

7.2 Percent (%) of external network traffic to/from the organization's networks that passes through a TIC/MTIPS.

100%

7.3 Percent (%) of external network/application interconnections to/from the organization's networks that passes through a TIC/MTIPS.

100%

7.4 Percent (%) of public-facing servers use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and Internet Service Provider (ISP) resources unless they require IPv6 to perform their business function.)

100%

Section 8: Training and Education

8.1 Percent (%) of users that successfully completed annual Cybersecurity Awareness and Training (CSAT).

97%

8.1.1 Percent (%) of new users who satisfactorily completed security awareness training before being granted network access or within an organizationally defined time limit that provides adequate security after being granted access.

80%

8.2 Percent (%) of all users that participated in cybersecurity-focused exercises.

100%

8.2.1 Percent (%) of the users in 8.2 that successfully completed exercises focusing on phishing, designed to increase awareness and/or measure effectiveness of previous training (e.g. organization conducts spoofed phishing emails, clicking link leads to phishing information page).

100%

8.3 Percent (%) of the organization's network users and other staff that have significant security responsibilities.

1%

8.3.1 Percent (%) of the personnel counted in question 8.3 that have successfully completing role-based security training within the reporting year.

95%

Section 9: Incident Response

Section 9: Incident Response

9.1 Of the information security incidents reported to US-CERT in FY2015, what was the total number of incidents reported to Congress?

0

9.2 Of all of the cyber related (electronic) incidents with confirmed loss of confidentiality, integrity or availability reported to US-CERT in FY15 (per OMB M-15-01), what was the average mean time (in hours) between detection and notification to the Agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or Information Technology (IT) department?

1.00

Comments:

In hours

9.3 When will the agency transition to the new US-CERT reporting format?

12/31/2014

Comments:

The agency has completed its transition in FY15 Q1 to the new US-CERT reporting format.



NOV 12 2015

MEMORANDUM

Date:

Refer To: S9

To: Robert Klopp
Chief Information Officer

From: Andy Liu
General Counsel

Subject: Senior Agency Official for Privacy (SAOP) Section Report for SSA's FY 2015 Federal Information Security Management Act (FISMA) Report to the Office of Management and Budget (OMB) – INFORMATION

OMB's FISMA FY 2015 privacy reporting instructions require that the Social Security Administration (SSA or agency) provide an SAOP privacy report. I have attached the FY 2015 SAOP privacy report for inclusion with the agency's FY 2015 FISMA report.

Additionally, OMB Memorandum M-16-03, entitled "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," requires the SAOP to submit the following documents:

- Description of the agency's privacy training for employees and contractors,
- Breach notification policy,
- Progress update on eliminating unnecessary use of Social Security Numbers,
- Progress update on the review and reduction of holdings of personally identifiable information, and
- A memorandum describing the agency's privacy program.

With regard to SSA's review and reduction of holdings of personally identifiable information, the attached SAOP privacy report states in response to Question 9a that OGC participated in agency activities to implement the requirements of OMB Memorandum M-07-16, entitled "Safeguarding Against and Responding to Breach of Personally Identifiable Information." Specifically, during FY 2015, OGC participated in an agency-wide annual review and reduction of all PII holdings. I have attached a September 19, 2015 memorandum documenting the completion of this review.

Please let me know if you have any questions. Your staff may address questions to Jasson Seiden, on extension 7-4307.

Attachments:

TAB A – FY 2015 SAOP Section Report

TAB B – Description of Agency Training for Employees and Contractors

TAB C – Agency Breach Notification Policy

TAB D – Update on Agency Efforts to Eliminate Unnecessary Use of SSNs

TAB E – FY 2015 OMB M-07-16 PII Review Memorandum

TAB F – Description of the Agency's Privacy Program

Senior Agency Official For Privacy

Section Report

2015
Annual
FISMA

Social Security Administration

Section 1: Information Security Systems

Agency/ Component	Submission Status	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 Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems
SSA	Submitted to Agency	21	0	21	18	0	18	18	0	18	21	0	21	21	0	21
Agency Totals		21	0	21	18	0	18	18	0	18	21	0	21	21	0	21

Section 2: 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/pia.html>
- 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/>

Section 3: 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.

- 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.

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

- 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 Systems 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.

Section 4: 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:

Our regulations (20 C.F.R. § 401.30(e)) provide that the SAOP ensure that employees and contractors receive training and education regarding privacy laws, regulations, policies, and procedures governing the agency's handling of personal information. We provide employees privacy education resources, and employees annually sign a sanctions document acknowledging their understanding of the penalties for misusing protected information. We also issue documentation to staff on safeguarding PII and adherence to the Privacy Act and other provisions. Our POMS, Chapter GN 033, contains instructions that apply to the disclosure of personal information in our records. In 2015, 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.

Section 4: 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:

We provide specialized training on the Privacy Act, and related privacy regulations, policies, and procedures. Employees have access to four specific VODs on protecting and safeguarding PII. In FY 2015, we continued our practice of training systems development staff on the importance of privacy and privacy risk assessment via the SDLC Configuration Control Board (CCB). By participating in the SDLC CCB, we review any proposed changes to lifecycle roles, activities, or work products that affect the administration of personal information and educate members on the importance of these activities. Additionally, both management and staff experts attend training conferences hosted by Privacy Interest Groups, OMB, and the CIO Council to ensure that their expertise remains current.

Section 5: PIA and Web Privacy Policies and Processes

Does the organization have a written policy or process for each of the following?

5a PIA Practices

5a(1) Determining whether a PIA is needed

Yes

5b Web Privacy Practices

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

Section 5: PIA and Web Privacy Policies and Processes

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 Management Directive 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.

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

Comments:

In accordance with federal mandates and policy, we continue to make many of our web pages machine-readable. Following requirements from the Open Data Policy and Digital Strategy, we make public data files, our public data listing, and our Digital Strategy road map available in machine-readable formats allowing the public and other government agencies the ability to harvest our information in an automated process. Even when making information available in a machine-readable format we continue to follow our Administrative Instructions Manual System (AIMS) (Chapter 15.01.05) requiring that we ensure compliance with rules and requirements concerning the protection of PII when making information available through our websites. We use content-aware compliance software to examine our webpages.

Section 6: Conduct of Mandated Reviews

Did your organization perform the following reviews as required by the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007? Indicate "N/A" if not applicable.

Agency/Component	a. Section (m) Contracts	b. Records Practices	c. Routine Uses	d. Exemptions	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
------------------	--------------------------	----------------------	-----------------	---------------	----------------------	-------------	-----------------------------	--------------------------------	------------------------------	---------------------	---	----------------------------------

Agency/Component	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	124	Y	X	X	103	80	49	X
TOTAL				3	124				103	80	49	

Section 7: Written Privacy Complaints

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

- 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
2
- 7d Referrals — complaints referred to another organization with jurisdiction
0

Section 8: 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.

Section 8: Policy Compliance Review

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:

To the extent that such oversight impacts records contained within the Inspector General's system of records or records in SSA's system of records maintained at the Inspector General's office locations, such as personal records of OIG employees.

Section 9: SAOP Advice and Guidance

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

9a 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 2015 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.

Section 9: SAOP Advice and Guidance

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.

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

Yes

Comments:

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

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

10a Does the 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.

Section 10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking 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 FY 2015.

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>.

10e Number of requests for Tier 3 web measurement and customization technologies approved by the SAOP during the reporting period (see OMB M-10-22 for more information)

0

Section 11: Information System Security

11a Number of authorizations to operate (ATOs) or reauthorizations issued during the reporting period

5

11b Number of ATOs or reauthorizations approved by the SAOP during the reporting period (OMB M-14-04 provided that SAOP approval is required as a precondition for the issuance of an ATO)

5

Section 12: Breach Response and Notification

Section 12: Breach Response and Notification

Pursuant to FISMA, each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems. New US-CERT Federal Incident Notification Guidelines are effective October 1, 2014.

12a	Number of confirmed breaches reported by your organization to the U.S. Computer Emergency Readiness Team (US-CERT) during the reporting period	4354
12b	Number of confirmed non-cyber related (e.g., paper) breaches experienced by your organization during the reporting period (OMB M-15-01 provided that non-cyber related incidents should be reported to your agency's privacy office and not to US-CERT)	3543
12c	Number of persons potentially affected by all confirmed breaches, both cyber and non-cyber, during the reporting period (approximate figures if precise figures are not available)	884962
12d	Number of potentially affected persons who were provided notification about a breach of information experienced by your organization that occurred during the reporting period	1438

FY 2015 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 2015, 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 2015, 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.

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

INQUIRES: Questions regarding the content of this issuance should be directed to [^OIS Controls@ssa.gov](mailto:OISControls@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.

- A. **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.
- B. **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.

15.6.12 [Attachment](#)

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

Social Security Administration

Important Information

Date:

NAME
MAILING ADDRESS
CITY ST ZIP CODE

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.*

FY 2015 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.
- Work closely with other Federal agencies in their continuing efforts to remove or eliminate the SSN from their documents. For example, we participate in a workgroup, led by the Department of Health and Human Services, to remove the SSN from the Medicare Card.



SOCIAL SECURITY


MEMORANDUM

Date: August 19, 2015

Refer To: SH9

To: Elizabeth Reich
Acting Deputy Commissioner
for Budget, Finance, Quality, and Management

Andy Liu
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) – 2015 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 2015 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 Navdeep Sarai (5-2997) of the Office of Privacy and Disclosure.

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

FY 2015 FISMA

Senior Agency Official for Privacy Report

Agency's Privacy Program Description

Social Security Administration's (SSA) Senior Agency Official for Privacy (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, such as the Privacy Act.

The SAOP's compliance efforts include reviewing information privacy policies and procedures to ensure that they are comprehensive and up-to-date and, where additional or revised policies and procedures may be called for, working with the relevant agency offices in considering, adopting, and implementing such procedures. The SAOP also ensures that agency employees and contractors receive appropriate training and educational programs regarding the information privacy laws, regulations, policies and procedures governing the agency's handling of personal information. In addition to the compliance role, the SAOP has a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals, which might implicate information privacy issues, including those relating to the collection, use, maintenance, and disclosure of personal information.

Working under the direction of the SAOP, SSA's Office of Privacy and Disclosure (OPD) ensures integration of privacy principles into all aspects of technology systems through an initial privacy assessment process. In our comprehensive review process, we incorporate the tenets of privacy law, SSA privacy regulations, and privacy policy directly into the development of certain information technology projects. Our review examines the risks and ramifications of collecting, maintaining, and disseminating information in identifiable form in an information system, and identifies and evaluates protections and alternate processes to reduce the risk of unauthorized disclosures. In addition, the initial privacy assessment may determine that a Privacy Impact Assessment, approved by the SAOP under 20 C.F.R. § 401.30, is required to assess the impact of the technology on protecting the privacy of personal information.

OPD, a component within the Office of the General Counsel and under the leadership of the SAOP, performs the compliance activities mentioned above. OPD has dedicated resources to perform the myriad of complex privacy-related functions. However, while we do have some dedicated resources, we are currently evaluating whether the resources are sufficient considering the abundance of new privacy-related reporting requirements from the Office of Management and Budget.

Inspector General

Section Report

2015

Annual FISMA
Report

Social Security Administration

MEMORANDUM

Date: November 12, 2015

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015 (A-14-16-50037)

The attached final report summarizes Grant Thornton LLP's (Grant Thornton) Fiscal Year (FY) 2015 audit of the Social Security Administration's (SSA) information security program and practices, as required by the *Federal Information Security Modernization Act of 2014* (FISMA).¹

FISMA requires that we, or an independent external auditor as determined by the Inspector General (IG), annually assess the effectiveness of SSA's information security policies, procedures, and practices.

Under a contract we monitored, Grant Thornton, an independent certified public accounting firm, audited SSA's compliance with FISMA for FY 2015. Grant Thornton's report, along with its responses to the FY 2015 IG FISMA reporting metrics developed by the Department of Homeland Security (DHS), are submitted through CyberScope pursuant to the Office of Management and Budget (OMB) Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management requirements*.

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 requirements of FISMA, 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, DHS, and the National Institute of Standards and Technology as well as SSA's 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.

¹ Pub. L. No. 113-283, 128 Stat. 3073 (2014).

Grant Thornton's Audit Results

Grant Thornton determined that, while SSA had established an overall information security program and practices that were generally consistent with the FISMA requirements, weaknesses in the following areas may have limited the program's effectiveness to adequately protect the Agency's information and information systems:

- Continuous Monitoring Management;
- Configuration Management;
- Identity and Access Management;
- Incident Response and Reporting;
- Risk Management;
- Security Training;
- Contingency Planning; and
- Contractor Systems.

Grant Thornton concluded that the risk and severity of the weaknesses they identified constituted a significant deficiency in internal controls over FISMA and as defined by OMB guidance.

OIG Comments

SSA houses sensitive information about nearly every U.S. citizen—living and deceased—including medical and financial records. Inappropriate and unauthorized access to, or theft of, this information can result in significant harm and distress to potentially hundreds of millions of Americans. As such, it is imperative that SSA make protecting its networks and information a top priority.

Since FY 2013, Grant Thornton has concluded that the risk and severity of the weaknesses they identified have constituted a significant deficiency with internal controls over FISMA and as defined by OMB guidance. Per OMB M-14-04, a significant deficiency is defined 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.²

In addition, our prior audits and evaluations identified serious concerns about SSA's information security program.

Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. We believe SSA must make protecting the Agency's networks and information systems a top priority and dedicate the resources needed to (1) ensure the appropriate design and operating effectiveness of information security controls and (2) prevent unauthorized access to the sensitive information the American public entrusts to SSA.

OIG Evaluation of Grant Thornton's Audit Performance

To fulfill our responsibilities under the *Inspector General Act of 1978*, we monitored Grant Thornton's performance audit of SSA's FY 2015 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 working papers;
- reviewing Grant Thornton's audit report to ensure it complies with government auditing standards;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

² OMB, M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013, page 8. To date, OMB has not released additional guidance on reporting of significant weaknesses nor additional definitions of deficiencies as it relates to FISMA.

Grant Thornton is responsible for the attached auditor's report and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton performance under the terms of the contract. Our review, as differentiated from an audit in accordance with applicable auditing standards, was not intended to enable us to express, and, accordingly, we do not express, an opinion about the effectiveness of SSA's information security policies, procedures, and practices. However, our monitoring review, as qualified 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 Rona Lawson, Deputy Assistant Inspector General for Audit, at (410) 965-9700.

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

Patrick P. O'Carroll, Jr.

Attachment



MEMORANDUM

Date: November 12, 2015

Refer To:

To: SSA Office of the Inspector General

From: Grant Thornton

Subject: The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015 (A-14-16-50037)

In conjunction with the audit of the Social Security Administration's (SSA) Fiscal Year (FY) 2015 Financial Statements, the Office of the Inspector General engaged us to conduct the performance audit on SSA's compliance with the *Federal Information Security Modernization Act of 2014* (FISMA) for FY 2015. The objective was to determine whether SSA's overall information security program and practices were effective and consistent with FISMA requirements, 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 SSA management, SSA's Office of the Inspector General, the Office of Management and Budget, the Government Accountability Office, and Congress and is not intended to, and should not, be used by anyone other than the specified parties.

A handwritten signature in black ink that reads "Grant Thornton LLP".

Alexandria, Virginia
October 30, 2015

The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015

A-14-16-50037

November 2015

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 Modernization Act of 2014* (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 (FY) 2015 FISMA performance audit in accordance with Government Auditing Standards. We assessed the effectiveness of SSA's information security controls including its 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 by performing additional testing procedures as needed. We used the DHS OIG FY 2015 Inspector General (IG) FISMA reporting metrics as the basis for our assessment of SSA's overall information security program and practices.

Findings

Although SSA had established an information security program and practices that were generally consistent with FISMA requirements, we identified a number of deficiencies related to continuous monitoring management; configuration management; identity and access management; incident response and reporting; risk management; security training; contingency planning; and contractor systems. Many of the weaknesses we identified were similar to the deficiencies reported in past FISMA assessments. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. We concluded that the risk and severity of the weaknesses constituted a significant deficiency in internal controls over FISMA and as defined by Office of Management and Budget (OMB) guidance, M-14-04.

Recommendations

While SSA continued executing its risk-based approach to strengthen controls over its information systems and address weaknesses during FY 2015, we identified persistent deficiencies in both the design and operation of controls related to the DHS reporting metrics. We believe that SSA must strengthen its information security risk management framework and enhance information technology (IT) oversight and governance to address these weaknesses. SSA must make the protection of the Agency's networks and information systems a top priority, and dedicate the resources needed to (1) ensure the appropriate design and operating effectiveness of information security controls and (2) prevent unauthorized access to the sensitive information. We provided detailed recommendations throughout the performance audit for each weakness identified. Additional recommendations can be found within the conclusions and recommendations section of this report.

SSA management generally agreed with the findings and recommendations, however, management disagreed with our assessment of compliance for some risk management metrics. Management responses and Grant Thornton's response can be found within the views of responsible officials section of this report.

TABLE OF CONTENTS

Objective	1
Background	1
Scope and Methodology	2
Results of Review	3
Significant Information Security Control Weaknesses	4
Configuration Management	4
Identity and Access Management	4
Risk Management	4
Security Training	5
Agency Efforts to Resolve Weaknesses and Potential Causes for the FY 2015 FISMA Significant Deficiency	6
Conclusions and Recommendations	6
Views of Responsible Officials	7
Grant Thornton Response	10
Appendix A – Scope and Methodology	A-1
Appendix B – Response to Fiscal Year 2015 Inspector General <i>Federal Information Security Modernization 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 – Acknowledgments.....	E-1

ABBREVIATIONS

ATO	Authorization to Operate
BCP	Business Continuity Plan
CIGIE	Council of Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CONOPS	Concept of Operations
CSP	Cloud Service Provider
DDS	Disability Determination Services
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	<i>Federal Information Security Modernization Act of 2014</i>
FSA	Financial Statement Audit
FY	Fiscal Year
GAO	Government Accountability Office
Grant Thornton	Grant Thornton LLP
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OIG	Office of the Inspector General
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
POMS	Program Operations Manual System
Pub. L. No.	Public Law Number
RMF	Risk Management Framework
RO	Regional Office

SA&A	Security Assessment and Authorization
SDLC	System Development Lifecycle
SP	Special Publication
SSA	Social Security Administration
SSP	System Security Plan
TT&E	Test, Training & Exercise
U.S.C.	United States Code
USGCB	United States Government Configuration Baseline

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 Modernization Act of 2014* (FISMA), as defined by the Department of Homeland Security (DHS).¹ 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

SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the FY 2015 FISMA performance audit in conjunction with the audit of SSA's Fiscal Year (FY) 2015 Financial Statements.² FISMA includes the following key requirements.

- Each agency must develop, document, and implement an agency-wide information security program.³
- 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.⁴
- 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.⁵

Generally, the requirements of the IG's independent evaluation remain unchanged over FISMA (as amended); however, DHS implemented changes in the evaluation guidance for the continuous monitoring management reporting metric. Specifically, the Information Technology Committee of the Council of Inspectors General on Integrity and Efficiency (CIGIE), in coordination with DHS, the Office of Management and Budget (OMB), the National Institute of

¹ The *Federal Information Security Modernization Act of 2014* amends the *Federal Information Security Management Act of 2002* Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014).

² OIG Contract Number GS-23F-8196H, December 3, 2009.

³ Pub. L. No. 113-283, § 2§ 3554(b); 44 U.S.C. § 3554(b).

⁴ Pub. L. No. 113-283, § 2 § 3554(a)(1)(A); 44 U.S.C. § 3554(a)(1)(A).

⁵ Pub. L. No. 113-283, § 2 §§ 3555(a)(1) and (b)(1); 44 U.S.C. §§ 3555(a)(1) and (b)(1).

Standards and Technology (NIST), and other key stakeholders, developed a maturity model to provide perspective on the overall status of information security within an agency as well as across agencies. For FY 2015, CIGIE started with a maturity model for the information security continuous monitoring (ISCM) domain. The model has five levels: ad-hoc, defined, consistently implemented, managed and measurable, and optimized. To reach a specific level of maturity, organizations must meet all of the attributes within that particular maturity level. SSA management communicated a self-assessment maturity level of defined for the FY 2015 FISMA evaluation. Therefore, we assessed SSA's ISCM program against the defined attributes for the ISCM program.

SCOPE AND METHODOLOGY

DHS issued 10 reporting metrics, dated June 19, 2015, for the IG's FY 2015 FISMA submission.⁶ The following DHS reporting metrics were included in the scope of the performance audit.

FY 2015 Inspector General FISMA Reporting Metrics

1. Continuous Monitoring Management⁷
2. Configuration Management
3. Identity and Access Management
4. Incident Response and Reporting
5. Risk Management
6. Security Training
7. Plan of Action & Milestones (POA&M)
8. Remote Access Management
9. Contingency Planning
10. Contractor Systems

We conducted our performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. We followed the Government Accountability Office's (GAO), *Federal Information System Controls Audit Manual*, which provides guidance for evaluating Electronic Data Processing general, and application controls in a Federal audit under generally accepted government auditing standards. We leveraged work performed as part of the FY 2015 Financial Statement Audit (FSA), conducted in accordance with generally

⁶ Metrics posted by DHS on e-Government Community Website
<http://www.dhs.gov/sites/default/files/publications/FY15%20IG%20Annual%20FISMA%20Metrics%201.2%20Final%20508.pdf>.

⁷ Metrics posted by DHS for FY 2015 for Continuous Monitoring Management are based on a 5-level maturity model scale. Continuous Monitoring Management was chosen as the first security domain to move to the maturity model with additional security domains moving to the maturity model in future years. This was included with the IG reporting metrics posted by DHS.

accepted government auditing standards, and performed additional procedures as required to assess the reporting metrics listed above.

This report informs those charged with governance about SSA's security performance, as required by FISMA, and fulfills OMB and DHS requirements over FISMA to submit an annual report to Congress. Refer to Appendix A for additional information on our scope and methodology.

RESULTS OF REVIEW

Although we determined that SSA had established an information security program and practices that were generally consistent with FISMA requirements, we identified a number of deficiencies related to continuous monitoring management; configuration management; identity and access management; incident response and reporting; risk management; security training; contingency planning; and contractor systems.⁸ The weaknesses identified may limit the Agency's ability to adequately protect the confidentiality, integrity, and availability of SSA's information systems and data.⁹ 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 concluded that the risk and severity of SSA's information security weaknesses, including those listed below, and other weaknesses outlined in Appendix B, were considered a significant deficiency in internal controls over FISMA and as defined by OMB guidance. OMB M-14-04 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

⁸ We based our conclusions on our assessment of the DHS' FY 2015 IG FISMA reporting metrics; refer to Appendix A for additional information on Scope and Methodology.

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. 113-283, § 2, §§ 3552(b)(3)(A) to (C), 44 U.S.C. §§ 3552(b)(3)(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. To date, OMB's definition of significant deficiency remains the same. OMB's *Fiscal Year (FY) 2015 Frequently Asked Questions on Reporting for the Federal Information Security Management Act and Agency Privacy Management*, page 15, provides the OMB's significant deficiency definition, <https://community.max.gov/x/eQPENw>.

Significant Information Security Control Weaknesses

Of the eight reporting metrics with overall issues, we cited significant information security control deficiencies within the areas of configuration management, identity and access management, risk management, and security training that resulted in negative conclusions associated with metrics tested.¹¹ Specifically we noted the following.

Configuration Management

- SSA's documentation did not provide sufficient risk analysis, justification, and approval for a significant number of deviations from United States Government Configuration Baseline (USGCB) secure configuration settings.
- We identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner, as specified in organization policy or standards.¹²

Identity and Access Management

- We identified numerous issues with logical access controls that resulted in inappropriate and/or unauthorized access, including application developers (programmers) with unmonitored access to production and application transactions, as well as, other users with inappropriate access to data, change management libraries, and other privileged functions/sensitive system software resources.
- We identified control failures related to the timely removal of terminated employees' logical access to the mainframe, network, and other supporting systems.
- SSA did not have an authoritative source to identify departure dates for individual contractors; therefore, the Agency was unable to supply actual departure dates for contractors to substantiate timely removal of their systems access.

Risk Management

- We identified information system control weaknesses for various non-central office sites that continue to persist from past audits because corrective actions have not been appropriately designed, planned, and/or implemented to remediate control weaknesses and mitigate risks.

¹¹ We provided Agency management with a Notice of Finding and Recommendation for weaknesses noted during the audit. The Notice of Finding and Recommendation included the condition, criteria, cause, effect, and recommendation(s).

¹² Because disclosing specific details about these weaknesses might further compromise controls, we provided those details to SSA in a separate, limited-distribution management letter.

Lack of a comprehensive governance structure and organization-wide risk management strategy, inconsistent implementation of SSA's information security program requirements, and a lack of sufficient IT assessments performed by Management continue to contribute to the control weaknesses identified. More significant control weaknesses include inadequate platform security, inadequate policy/procedural guidance, and inadequate development and execution of a risk management framework (RMF) aligned with the NIST criteria.

- We noted SSA had not applied its RMF across all decentralized systems; as such, not all information systems had formal system security plans (SSP) or were mapped to an existing boundary with an SSP. Therefore, appropriately tailored sets of baseline security controls were not determined (or identified) and documented across all systems. In addition, we noted inconsistencies with documentation and implementation of common controls, hybrid controls, and system specific controls based on our reviews of entity level SSPs and information system specific SSPs.
- We noted that, without appropriately selected and documented sets of controls and assessments, the security controls may not be implemented as intended. Further, without consistency in mapping of common, hybrid, and system-specific controls, implementation of such controls may not be appropriate.
- SSA had not applied its RMF requirements across all decentralized systems. Consequently, security controls may not be appropriately assessed, and information systems may be in operation without an authorization to operate (ATO).
- SSA adopted the NIST definition of cloud computing models; however, testing indicated that SSA had not reviewed potential cloud based systems to appropriately identify those that meet the NIST definition. In addition, processes had not been established to periodically review a listing of cloud systems to ensure the Agency's portfolio of cloud systems remains complete and accurate.
- SSA developed a process during the audit period to identify security control requirements and to review FedRAMP SA&A artifacts for CSPs. The process had been executed for one specific CSP; however, for two other information systems identified by SSA as meeting the NIST cloud computing definition, FedRAMP requirements had not been met, therefore, risks may not be appropriately managed.

Security Training

- SSA did not have an authoritative system to identify and track completion of security awareness training for all employees and contractors.
- We noted numerous instances where evidence was not available to substantiate the completion of training for employees and contractors.

Agency Efforts to Resolve Weaknesses and Potential Causes for the FY 2015 FISMA Significant Deficiency

While SSA continued executing its risk-based approach to strengthen controls over its systems and address weaknesses in FY 2015, our testing identified issues in both the design and operation of controls that were similar to those we cited in our FY 2014 FISMA report.¹³ We believe that, in many cases, these deficiencies continued to exist because of one, or a combination, of the following.

- Risk mitigation strategies and related control enhancements required additional time to be fully implemented or become fully effective throughout the environment.
- SSA focused its limited resources on higher risk weaknesses and therefore was unable to implement corrective action for all aspects of the prior year deficiencies.
- The design of enhanced or newly designed controls did not completely address risks and recommendations provided over past audits.
- Oversight and governance were not sufficient.

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

CONCLUSIONS AND RECOMMENDATIONS

Although SSA had established an information security program and practices that were generally consistent with FISMA requirements, we identified a number of deficiencies related to continuous monitoring management; configuration management; identity and access management; incident response and reporting; risk management; security training; contingency planning; and contractor systems. Many of the weaknesses we identified were similar to the deficiencies reported in past FISMA assessments. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. We concluded that the risk and severity of the weaknesses we identified constituted a significant deficiency in internal controls over FISMA and as defined by OMB M-14-04.

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 we identified could negatively impact the confidentiality, integrity, and availability of the Agency's systems and data. We believe that SSA must strengthen its information security risk management framework and enhance information technology oversight and governance to address these weaknesses.

¹³ *The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014* (A-14-14-24083), October 31, 2014.

SSA must make the protection of the Agency's networks and information systems a top priority, and dedicate the resources needed to (1) ensure the appropriate design and operating effectiveness of information security controls and (2) prevent unauthorized access to the sensitive information. SSA should implement the following recommendations, as well as, additional recommendations provided throughout the performance audit in our NFRs:

- Implement requirements or complete sufficient risk analysis, justification, and approval(s) for security configuration deviations including, but not limited to, those associated with the USGCB for Windows components.
- Continue, as part of the SSA threat and vulnerability management processes, prioritization and implementation of risk mitigation strategies and POA&Ms.
- Analyze account management controls including access authorization, recertification, and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and oversight of processes.
- Continue, as part of the Cybersecurity Sprint initiative, to improve controls over privileged accounts.
- Continue, as part of the SSA profile quality program, additional profile content reviews and profile improvement initiatives.
- Enhance current information technology oversight and governance processes to ensure SSA information technology risk management framework requirements, as they apply to SSA, cloud, and contractor systems, are effectively and consistently implemented across the organization.
- Address security awareness training weaknesses identified as well as other weaknesses noted within the comments of Appendix B by implementing our recommendations provided throughout the audit.

VIEWS OF RESPONSIBLE OFFICIALS

We discussed our conclusions with SSA officials who generally agreed with our findings and recommendations. However, in relation to the risk management metrics, SSA disagreed with our assessment of compliance for some metrics. Specifically, SSA provided the following formal response:

Thank you for the opportunity to respond to the draft FISMA audit report. The Agency appreciates the effort to assess our compliance with the FISMA controls and to provide us feedback. We disagree with the reduced compliance metrics in the area of Risk Management. SSA takes seriously our responsibility to protect the information and technology that we use to administer our programs. For the FY 2015 FISMA audit, Grant Thornton determined that we established an information security program and practices that were generally consistent with FISMA requirements. We make ongoing

improvements to our risk management protocols to keep pace with changes in the operating environment, mitigate known risks, and address prior audit recommendations. Throughout this audit we have engaged Grant Thornton to explain our approach, provide documentation of our progress, and obtain feedback on their assessment. In FY2015, Grant Thornton noted that we made substantial improvements and progress in securing applications and managing vulnerabilities for the vast majority of our systems resources. We improved our existing controls in addition to implementing new controls and risk management processes in FY 2015, yet our overall score was lowered from what was reported in FY 2014. We have completed action on many recommendations from the FY2014 FISMA assessment, and continue to address open recommendations. Following best practices and to make the best use of limited resources, we prioritize our actions for improvement to address the most significant risks first. For example, in FY2015 we reduced the number of privileged accounts, increased the number of individuals who use Personal Identify Verification (PIV) cards, expanded our penetration testing program to include external testing, added additional cyber hygiene scans, and published an agency wide change management directive that defines the change policy for all SSA developed applications, including regional ones.

Grant Thornton indicated that risk management compliance decreased because there are an extensive number of applications hosted at decentralized locations. Their discussions revealed the number may include or exceed 600 applications. These findings extend to disability case processing systems that are hosted at DDS locations. However, in FY 2015 we improved our controls on these decentralized applications. As part of a multi-year effort to extend our robust risk management protocols to all decentralized software applications we have begun a Security Assessment and Authorization (SA&A) process for regionally developed applications. As of the end of FY2015 we had assessed risk for the distributed software applications specifically identified by Grant Thornton in FY 2014 and 2015. We have increased our staffing to the SA&A area to accelerate the roll out of the standard regional SA&A process. In addition, the agency:

- Assessed the risk associated with these applications as low because regional applications are smaller in scope and do not process programmatic or financial transactions. They are not tied to financial systems. Almost 300 of these “applications” are region-specific tools that do not contain personal information, e.g., spreadsheets or static SharePoint sites. Due to the lack of financial impact or significance, we consider these applications lower risk. There are existing regional oversight processes to manage risk in these applications until we develop the standardized SA&A process.
- Extended our mature and robust process for assessing the security of our mission-critical systems to include our decentralized applications. The newly developed SA&A process for regionally developed applications, includes assigning the 600+ applications to security authorization boundaries as well as documenting and assessing the security controls in place. We plan to fully implement this process by Q1 of FY16. We developed this process for managing security risks in a comprehensive and consistent manner for applications developed in our regions.

While we did not fully implement the SA&A process in FY15, we made significant progress, including the development of a complete and accurate inventory. With these additional improvements, our compliance and scores for the FISMA metrics should not have decreased over the prior year.

- Standardized system security plans for DDSs and continued to improve governance and oversight over DDS processes. We manage contracts to operate, change, and replace DDS systems. Through these contracts we maintain oversight, control, and monitoring of DDS systems. We have security risk configuration standards and scans for the DDS systems. We will continue to improve in this area, and in FY2015 our compliance improved over 2014 with the implementation of the security plans and changes to disability security policies. Additionally, governance over the DDS systems will be greatly enhanced with the implementation of the Disability Case Processing System (DCPS) in FY 2016. DCPS will provide standard system infrastructure for all DDS processes.

Grant Thornton assessed information security for a selection of decentralized systems and cited weaknesses similar to those identified in past audits. Specifically, recurring issues continued to be cited with security management, physical and logical access controls, and platform security.

- The findings that Grant Thornton cites as recurring are minor documentation issues; examples include references to incomplete checklists and references to code documentation for a system that is 30 years old. Following best practices and to make the best use of limited resources, we take a risk based approach to addressing findings and we consider these types of documentation findings to be low risk issues. We prioritized our FY2015 improvements to address issues identified as higher risk. We will continue to standardize and improve our documentation.
- In FY 2015 we implemented the electronic form-120 to improve access control to SSA systems resources and by Q1 FY16, will implement the Security Access Management (SAM) workflow tool which will further improve the control of access to systems resources.

Grant Thornton noted that we did not follow our policy in relationship to FedRAMP for cloud applications. During FY 2015, we authorized the use of Amazon Web Services for agile development and testing by following Federal Risk Authorization and Management Program (FedRAMP) requirements. This was a substantial improvement in our cloud infrastructure. We are following our policy for all cloud applications that are classified as cloud implementations per the NIST definition, that FedRAMP references. We believe this finding is the result of not fully and accurately assessing work done during the course of the fiscal year.

In conclusion, SSA practices a defense in depth cyber strategy that employs a strong set of security controls, technologies, policies and procedures to manage risk. We continuously improve our processes and controls to address the ever changing threat environment and escalating risks. Thank you again for the opportunity to respond to the draft FISMA audit report.

GRANT THORNTON RESPONSE

We appreciate the Agency's support throughout the FISMA audit, their diligence in reviewing the results of our FISMA audit, and their views as expressed above. We have evaluated the response and continue to disagree with their perspectives on our conclusions in the area of risk management. In FY 2015 we noted, within our independent auditor's report,¹⁴ that SSA continues to make progress in strengthening controls over its information systems to address the significant deficiency reported in FY 2014. However, in both that report and within this report, we also noted that while SSA continued executing its risk-based approach to strengthen controls over its systems and address weaknesses in FY 2015, our testing identified issues in both the design and operation of controls that were similar to those we cited in our FY 2014 audits. We worked closely with SSA throughout the audit period of 10/1/2014 to 9/30/2015 to discuss their approach to remediation, progress, and to provide feedback. However, substantial remedial activities were either not completed within the audit period or our testing results demonstrated that corrective action required more time to be fully implemented or become fully effective throughout the environment. This was further demonstrated in the results of this report, which are similar to those of the FY 2014 report. In response to SSA's above comments, we noted the following:

- Regarding vulnerability management, while areas of improvement were identified, testing continued to reveal weaknesses. As noted in metric 2.1.8, our information security and penetration testing, vulnerability management, and configuration management assessments identified control weaknesses with cyber/network security controls, many of which continue to exist from past audits.
- Regarding the risk management results, as SSA indicated, our conclusions for many metrics in FY 2015 were cited as a "no" compared to a "yes" in FY 2014. We expanded our scope in FY 2015 based on findings from our prior year report to include additional testing of a second region and we performed additional inquiry to assess SSA's implementation of risk management activities throughout the regions and the DDS sites. In our discussions with SSA we learned that the DDS case processing systems and potentially over 600 regional office applications had not been subjected to risk management activities, i.e. SA&A. Further, during the audit period, SSA was still in the process of completing SA&A activities for the two regional applications selected for testing. The results from our increased scope revealed

¹⁴ Grant Thornton, Independent Auditor's Report on SSA's FY 2015 financial statements will be released in November 2014.

pervasive issues across decentralized locations and systems. As SSA notes in its response, this is a multi-year effort to extend its risk management protocols to decentralized locations. While an inventory was created and a process developed to complete SA&A activities, the vast majority of corrective actions were not completed in this audit period and therefore could not be assessed. This is based on SSA's statement that the newly developed SA&A process will not be fully implemented until Q1 FY 2016.

- Regarding the risk associated with the applications, SSA stated that a risk assessment was completed and the regional applications were determined to be low risk. However, FISMA requirements extend beyond financial and mission-critical systems; security requirements should be implemented across an organization. Information system weaknesses, even in lower risk applications and supporting systems, can lead to exposures that may impact financial or mission-critical data and/or result in data loss. Further, these findings extend to disability case processing systems that are hosted at DDS locations. These systems play a significant role in benefit processing for disability claims and should be considered major applications.
- Regarding the DDS sites, SSA had not fully implemented the standardized security plan during our audit period and we continued to identify platform security concerns across the DDS sites visited in FY 2015. DCPS was also not applicable to the current audit period.
- Regarding the recurring issues identified in our field work, we believe these are indicative of a lack of oversight and governance. Numerous issues continue to persist from past audits and minimal corrective action had been taken through the audit period to address the findings. For example, platform security issues for the DDS sites have been reported in management letter comments to the Agency dating back to 2004. Further, in response to SSA's comments on recurring issues:
 - Security Management – Issues cited in the current year included weaknesses in performance of background checks and a lack of comprehensive and approved system security plans. In addition, we continued to note areas where SSA's security requirements/guidance to DDSs was ambiguous, inconsistent, or not sufficiently documented. An appropriate security management program and system security plans afford management the opportunity to provide appropriate direction and oversight of the design, development, and operation of critical system controls. Lack of appropriate controls may result in inconsistent implementation and application of security measures.
 - Physical and Logical Access – Issues cited in the current year included weaknesses in performance of physical access recertification, inappropriate physical access to sensitive areas, terminated individuals retaining physical access to sensitive areas, as well as, logical access, and issues with logical access authorization. The electronic form-120 did not reduce the types of issues identified in past years and SAM was not implemented during the audit period.

- Platform Security – SSA discussed its security risk configuration standards and scans for the DDS systems. However, our testing continued to identify weaknesses in the platform security of decentralized sites tested. In regards to the DDSs, we identified weaknesses in reviewing compliance against SSA’s risk configuration standards, configurations on the platforms not aligned with SSA’s standards, a lack of reviews over inactive accounts, a lack of evidence to support reviews of users with privileged access, instances of inappropriate access to sensitive accounts, and instances of weak credentials. Finally, we noted issues associated with vendor account management and audit logging/monitoring.
- Regarding cloud systems, our assessment focused on information systems that SSA stated met its definition of cloud computing models (please note SSA adopted the NIST definition of cloud computing models). For systems we tested, SSA had not met FedRAMP requirements, contrary to the Agency’s documented policy/procedures. Specifically, SSA requirements stated, “SSA will only use FedRAMP evaluated and compliant cloud service providers (CSP). If the cloud system is not FedRAMP compliant and was built by an external private sector CSP, the agency should inform the CSP that the system is not FedRAMP compliant, and advise the CSP that FedRAMP requirements should have been met by June 5, 2014.”

Given the increased risks identified from our expanded scope in FY 2015, and as a result of these weaknesses and others detailed outlined in Appendix B, we believe our results support our conclusions in the risk management area.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Modernization Act of 2014* (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 objective of Grant Thornton LLP's (Grant Thornton) audit was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the FISMA requirements, as defined by the Department of Homeland Security (DHS). Annually, DHS publishes reporting metrics to be utilized as the basis for this assessment. SSA's IG contracted with us, Grant Thornton, to audit SSA's Fiscal Year (FY) 2015 financial statements and perform the FY 2015 FISMA performance audit. 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* to leverage testing performed during the SSA FSA. 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. We assessed information systems internal controls, as they were significant to the audit objectives and DHS IG reporting metrics, using Federal Information System Controls Audit Manual guidance including performance of inquiry, observation, and inspection procedures.

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

- FISMA law;
- Office of Management and Budget (OMB) guidance, including OMB Memorandum 16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*;
- DHS annual FISMA reporting instructions and annual FISMA IG reporting metrics, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics* V1.22.
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources;

¹ Pub. L. No. 113-283, § 2, §§ 3555(a)(1), (a)(2)(A), (a)(2)(B); and (b)(1), 44 U.S.C. §§ 3555(a)(1) (a)(2)(A), (a)(2)(B); and (b)(1).

² <http://www.dhs.gov/sites/default/files/publications/FY15%20IG%20Annual%20FISMA%20Metrics%201.2%20Final%20508.pdf>.

- Standards and guidelines issued by the National Institute of Standards and Technology (NIST) – including, NIST Special Publication 800-53 Revision 4 *Security and Privacy 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 of Federal Employees and Contractors*; and other NIST publications cited in DHS’ annual FISMA IG reporting metrics;
- Other Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics; and,
- Applicable SSA policies.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives.

Appendix B – RESPONSE TO FISCAL YEAR 2015 INSPECTOR GENERAL *FEDERAL INFORMATION SECURITY MODERNIZATION ACT* REPORTING METRICS

Section 1: CONTINUOUS MONITORING MANAGEMENT

1.1. Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.

1.1.1. Please provide the D/A ISCM maturity level for the People domain.

Level 2 - Defined

1.1.2. Please provide the D/A ISCM maturity level for the Processes domain.

Level 2 - Defined

1.1.3. Please provide the D/A ISCM maturity level for the Technology domain.

Level 2 – Defined

- Although the organization has already started to implement the first phase of the ISCM strategy, we noted that SSA continues to rely on manual / procedural methods in instances where automation may be more effective. Some future automation includes enhancements to network access control, configuration management, and patch management.

1.1.4. Please provide the D/A ISCM maturity level for the ISCM Program Overall.

Level 2 – Defined

- We noted that SSA continued enhancing automated continuous monitoring capabilities in fiscal year (FY) 2015. Further, SSA developed a plan to transition from its current 3-year re-authorization cycle to a time- and event-driven security authorization process. The current transition timeline, as documented in the ISCM strategy, noted conversion to ongoing authorization to be completed by FY 2018.

1.2. Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.

- We noted that resources (people, processes, and tools) were defined associated with ISCM activities across the organization; however, the policies and procedures were not consistently implemented. Specifically, we noted a lack of IT oversight and governance, inconsistent implementation of SSA's information security program requirements, and a lack of sufficient IT assessments performed by Management that continue to contribute to the control weaknesses identified at non-central office sites

and for decentralized systems. Further, this indicates that the Agency did not consistently integrate its ISCM and risk management activities.

- We noted inconsistencies in the processes associated with security configuration monitoring / management and monitoring of audit logs for decentralized information systems.

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?

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: We noted SSA documented an Agency-wide directive related to change management requirements for Agency application software supporting core business functions; however, not all procedures related to processes and control activities to meet requirements were finalized. Further, we continue to note that SSA's system software change processes did not require comprehensive security impact analysis for all changes, testing requirements based on risk, and requirements for the review and approval of testing results.

2.1.2. Defined standard baseline configurations. (Base)

FY 2015 Conclusion: Yes

Comments: We noted that SSA established a list of authorized infrastructure software (platforms) and developed standard baseline configurations for authorized platforms. However, we noted instances where the Agency's configurations deviated from standards and/or best practices without appropriate risk analysis, justification, and approval(s).

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

FY 2015 Conclusion: Yes

Comments: While evidence supported that security baseline configuration reviews were generally performed, we noted instances where assessments of compliance with baseline configurations were not adequately documented. In addition, we noted instances where configurations within the environment deviated from SSA's established configuration standard and/or best practices without appropriate risk analysis, justification, and approval(s).

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

FY 2015 Conclusion: Yes

Comments: We noted that SSA had processes in place for remediation of security weaknesses identified through SSA's scanning and internal penetration testing. However, our testing identified network security issues indicating potential weaknesses with the design of institutionalized control processes and/or lack of effectuation of the controls throughout the environment intended to mitigate such risk.

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

FY 2015 Conclusion: No

Comments: Documentation for a significant number of Windows (specifically Windows 7 and Vista) deviations from the USGCB settings did not provide sufficient risk analysis, justification, and approval(s) for the deviations.

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

FY 2015 Conclusion: Yes

Comments: While we noted that proposed and actual changes were generally identified and documented, our testing identified system software documentation weaknesses including a lack of completion of security impact / risk assessments, test plans, and retention of testing output. For application changes, we noted instances where there was a lack of evidence to support security impact analysis, testing and other requirements such as approvals.

2.1.7. Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI-2). (Base)

FY 2015 Conclusion: Yes

Comments: N/A

2.1.8. 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)

FY 2015 Conclusion: No

Comments: During our testing of threat and vulnerability management processes, we identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner, as specified in organization policy or standards. Specific disclosure of detailed information about these weaknesses might further

compromise controls and are therefore not provided within this report. Rather, the specific details are presented in a separate, limited-distribution management letter.

2.1.9. Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2). (Base)

FY 2015 Conclusion: Yes

Comments: While the platforms we selected for testing were appropriately patched, we noted for some de-centralized systems that localized procedures for patch management processes were not documented.

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: We noted that software and platforms that were approved for use only by specific "projects" required approval from the Architecture Review Board (ARB) prior to being implemented into production. Per inquiry, the Agency required that a security baseline be documented for any software approved for use as part of a software development project. However, we noted that there were no requirements to periodically monitor the software for compliance with the baseline. Additionally, these processes were not formally documented in a policy or procedure.

2.3. Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability? (Base)

FY 2015 Conclusion: Yes

Comments: We noted that SSA identified deviations to software through configuration management, patch management, and vulnerability management processes. In addition, SSA developed an exception reporting process and the security exception request form. However, the Agency did not consistently provide sufficient risk analysis, justification, and approval(s) when configuration baselines deviated from Federal standards and/or best practices and when configurations in the environment deviated from SSA's standard. This was noted for USGCB deviations and other platforms selected for testing.

2.3.1. Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorization departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented. (Base)

FY 2015 Conclusion: Yes

Comments: Refer to comments for 2.3.

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?

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: As part of our site visits and platform assessments, we noted instances where localized procedures for physical and/or logical account management processes and controls were not documented or required enhancements.

3.1.2. Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2). (Base)

FY 2015 Conclusion: Yes

Comments: Although the Agency was able to identify all users, including contractors, with access to the mainframe and all user accounts with access to the network, our testing identified weaknesses related to the appropriate completion of authorization forms for new hires, transferred employees, and contractors.

3.1.3. 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)

FY 2015 Conclusion: Yes

Comments: N/A

3.1.4. 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).

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: No

Comments: We identified numerous issues with logical access controls including adequate completion of approval forms for new and transferred information system users, recertification processes, and with the timely removal of logical access which may have contributed to instances of inappropriate and/or unauthorized

access identified as part of testing. This includes, but may not be limited to, application developers (programmers) with unmonitored access to production and application transactions, as well as, other users with inappropriate access to data, change management libraries, and other privileged functions/sensitive system software resources.

3.1.6. Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers). (Base)

FY 2015 Conclusion: Yes

Comments: N/A

3.1.7. Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy. (Base)

FY 2015 Conclusion: No

Comments: We identified control failures related to the timely removal of terminated employees' logical access to the mainframe, network, and other supporting systems. Additionally, SSA did not have an authoritative source to identify departure dates for individual contractors and therefore, SSA was unable to supply actual departure dates for contractors to substantiate timely removal of access.

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

FY 2015 Conclusion: Yes

Comments: N/A

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: We noted the following:

- As part of site visits, a non-central office location did not meet SSA's background check requirements. Further, we noted instances where suitability requirements were not met for individuals prior to gaining access to SSA's systems/facilities. In addition, these findings indicate that while SSA took correct action to address findings noted in the OIG Audit Report A-15-13-13092, *Contractor Access to Social Security Administration Data*, remedial actions may not have addressed root causes.
- SSA did not perform a comprehensive access review for platform administrative accounts. Further, we noted that recertification processes did not require the review of non-user accounts (e.g. service accounts, machine accounts, shared accounts, etc.).

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?**

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: Based on inquiry, SSA adopted United States Computer Emergency Readiness Team (US-CERT) timeframes for reporting of cyber incidents; however, had not documented the US-CERT reporting timeframes within their policy / procedure.

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

FY 2015 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)**

FY 2015 Conclusion: Yes

Comments: For a selection of cybersecurity incidents reported to US-CERT, we noted many instances where the incidents were not reported in a timely manner; however, the vast majority (all but one in our sample) occurred prior to SSA implementing formal procedures during the audit period. Further, we noted, for our selection of Personal Identifiable Information (PII) incidents, that SSA reported the incident to US-CERT within one hour of confirmation. However, we noted inconsistency in the amount of time it took SSA to review and confirm PII incidents after being made aware of the potential incident; the time period ranging from minutes to 20 days. While it is expected that some incidents may take longer to confirm, without documented requirements or guidance around the timeliness of review there may be great inconsistency in the actual timeframes to confirm an incident.

- 4.1.4. When applicable, reports to law enforcement and the agency Inspector General within established timeframes. (KFM)**

FY 2015 Conclusion: Yes

Comments: Refer to comments in 4.1.3 above regarding reporting of PII incidents.

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

FY 2015 Conclusion: Yes

Comments: We noted that one incident selected for testing did not have the Agency's resolution/analysis documented.

4.1.6. Is capable of correlating incidents. (Base)

FY 2015 Conclusion: Yes

Comments: N/A

4.1.7. 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)

FY 2015 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.

FY 2015 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?

FY 2015 Conclusion: Yes

5.1.1. 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. (Base)

FY 2015 Conclusion: No

Comments: As part of site visit testing, we identified weaknesses that continue to persist from past audits because corrective actions have not been appropriately designed, planned, and/or implemented to remediate control weaknesses and mitigate risks. Lack of a comprehensive governance structure and organization-wide risk management strategy, inconsistent implementation of SSA's information security program requirements, and a lack of sufficient IT assessments performed by Management, continue to contribute to the control weaknesses identified. More significant control weaknesses include inadequate platform security, inadequate policy/procedural guidance, and inadequate

development and execution of a risk management framework (RMF) aligned with the NIST criteria.

5.1.2. 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)

FY 2015 Conclusion: Yes

Comments: N/A

5.1.3. 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. (Base)

FY 2015 Conclusion: Yes

Comments: While we noted SSA developed an overall RMF for information systems and applied requirements to mission critical systems, the RMF was not consistently applied across decentralized organizations such as Regional Offices (RO) and Disability Determination Services (DDS).

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

FY 2015 Conclusion: Yes

Comments: We noted that SSA did not include RO and all DDS applications within its FISMA system inventory; however, the RO systems were included within a regional inventory system. In addition, we noted some inaccuracies within SSA's system inventory.

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

FY 2015 Conclusion: Yes

Comments: We noted that the majority of SSA's information systems were similarly categorized. However, SSA had not applied its RMF requirements across all decentralized systems, as such, not all information system's security categorizations were documented.

5.1.6. Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)

FY 2015 Conclusion: No

Comments: We noted SSA had not applied its RMF across all decentralized systems, as such, not all information systems had formal system security plans (SSP) or were mapped to an existing boundary with an SSP. Therefore, appropriately tailored sets of baseline security controls were not determined (or identified) and documented across all systems. In addition, we noted inconsistencies with documentation and implementation of common controls,

hybrid controls, and system specific controls based on our reviews of entity level SSPs and information system specific SSPs.

5.1.7. Implements the approved set of tailored baseline security controls specified in metric 5.1.6. (Base)

FY 2015 Conclusion: No

Comments: Refer to comments in 5.1.6 and 5.1.8. We noted that without an appropriately selected and documented set of controls and assessments the security controls might not be implemented or operating as intended. Further, without consistency in mapping of common, hybrid, and system specific controls implementation of such controls may not be appropriate.

5.1.8. Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)

FY 2015 Conclusion: No

Comments: We noted SSA had not applied its RMF requirements across all decentralized systems, as such; security controls may not be appropriately assessed.

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

FY 2015 Conclusion: No

Comments: We noted SSA had not applied its RMF requirements across all decentralized systems, as such; information systems may be in operation without an authorization to operate (ATO).

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

5.1.12. 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)

FY 2015 Conclusion: Yes

Comments: N/A

5.1.13. Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37). (Base)

FY 2015 Conclusion: Yes

Comments: We noted the mission-critical information systems security authorization packages contained appropriate artifacts. However, SSA did not consistently apply RMF requirements including Security Assessment and Authorization (SA&A) processes, which include development of system security plans, security assessments, and development of POA&Ms.

5.1.14. The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.

FY 2015 Conclusion: No

Comments: We noted SSA adopted the NIST definition of cloud computing models; however, testing indicated that SSA had not reviewed potential cloud based systems to appropriately identify those that meet the NIST definition. In addition, processes had not been established to periodically review a listing of cloud systems to ensure the portfolio of cloud systems remains complete and accurate.

5.1.15. For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.

FY 2015 Conclusion: No

Comments: We noted the Agency had developed a process during the audit period to identify security control requirements and to review FedRAMP SA&A artifacts for CSPs. The process had been executed for one specific CSP; however, for two other information systems identified by SSA as meeting the NIST cloud computing definition, FedRAMP requirements had not been met as of June 5, 2014. Therefore, risks may not be appropriately managed.

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.

FY 2015 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?

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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)

FY 2015 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)

FY 2015 Conclusion: No

Comments: We noted that SSA did not have an authoritative system to identify and track completion of security awareness training for all employees and contractors. In addition, we noted numerous instances where evidence was not available to substantiate the completion of training for employees and contractors.

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)

FY 2015 Conclusion: Yes

Comments: We noted instances where users selected for testing did not complete training that corresponded to their job responsibilities and/or where evidence did not support completion of required training hours. In addition, while SSA required that individuals with significant information security responsibilities track their own training, we noted that SSA did not have an Agency-wide or comprehensive

tracking system for all employees and contractors with significant information security responsibilities.

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

FY 2015 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?

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

7.1.4. Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates. (Base)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

7.1.7. Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25). (Base)

FY 2015 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: CA-5; OMB M-04-25). (Base)

FY 2015 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.

FY 2015 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?

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

8.1.7. 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

8.1.10. 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)

FY 2015 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.

FY 2015 Comments: N/A

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

FY 2015 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?

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: We noted that SSA incorporated results of its enterprise BIA into its COOP and DRP. However, SSA did not consistently require or document BIAs for newly developed applications and significant changes to existing applications. Therefore, the organization may be unaware should a new application or significant change to existing applications require more stringent recovery objectives. In addition, weaknesses associated with regional office applications may indicate that recovery objectives for these systems were not taken into account.

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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.

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

FY 2015 Conclusion: Yes

Comments: N/A

9.1.9. Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

9.1.11. Contingency planning that considers supply chain threats. (Base)

FY 2015 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.

FY 2015 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 for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

FY 2015 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 other government agencies), including organization systems and services residing in a public, hybrid, or private cloud. (Base)

FY 2015 Conclusion: Yes

Comments: While the Agency has policies and procedures relating to contractor systems, we noted SSA adopted the NIST definition of cloud computing models; however, testing indicated that SSA had not reviewed potential cloud based systems to appropriately identify those that meet the NIST definition. In addition, processes had not been established to periodically review a listing of cloud systems to ensure the portfolio of cloud systems remains complete and accurate.

10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2). (Base)

FY 2015 Conclusion: Yes

Comments: We noted that SSA generally identified contractor systems, but did not consistently obtain assurance that security controls and FISMA requirements were effectively implemented for contractor systems selected for testing. Specifically,

we noted instances of incomplete or missing SSPs, Authority to Operate (ATO) letters, and Business Continuity Plan (BCP).

10.1.3. A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in a public cloud. (Base)

FY 2015 Conclusion: Yes

Comments: While we noted SSA generally maintained a complete FISMA information system inventory, which included external systems, we noted that SSA did not differentiate cloud systems from external systems.

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

FY 2015 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)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 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.

FY 2015 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 System	HRS
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	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
5	Supplemental Security Income Record Maintenance System	SSIRMS
6	Social Security Number Establishment and Correction System	SSNECS
7	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 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 “[t]he program and supporting process to manage risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.” NIST Special Publication 800-53, Rev. 4, page B-11.19.
- **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.

Appendix E – ACKNOWLEDGMENTS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Principal, Grant Thornton

Cal Bassford, Senior Manager, Grant Thornton

Olga Mason, Manager, Grant Thornton

John O'Brien, Manager, Grant Thornton

Jessica Saunders, Manager, Grant Thornton

Kirsten Orr, Senior Associate, Grant Thornton

Kevin Potter, Senior Associate, Grant Thornton

Mitali Surti, Senior Associate, Grant Thornton