OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014

A-14-14-24083 | October 2014

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: October 31, 2014 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014 (A-14-14-24083)

The attached final report summarizes Grant Thornton LLP's (Grant Thornton) Fiscal Year (FY) 2014 audit of the Social Security Administration's (SSA) information security program and practices, as required by Title III of the *E-Government Act of 2002*, Public Law Number 107-347. Title III is also known as the *Federal Information Security Management Act of 2002* (FISMA).

FISMA requires that we, or an independent external auditor as determined by the Inspector General (IG), perform an annual evaluation that includes

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

Under a contract we monitored, Grant Thornton, an independent certified public accounting firm, audited SSA's compliance with FISMA for FY 2014. Grant Thornton's report, along with its responses to the FY 2014 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-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*.

Objective, Scope, and Methodology

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

Grant Thornton conducted its performance audit in accordance with generally accepted government auditing standards. Those standards require that Grant Thornton plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives.

Audit Results

For FY 2014, Grant Thornton determined that SSA had established an overall information security program and practices that were generally consistent with the FISMA requirements. However, identified weaknesses limited the program's effectiveness to adequately protect the Agency's information and information systems. Grant Thornton concluded that each of the Agency's metrics was generally consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology standards. However, Grant Thornton identified weaknesses in 8 of 11 metrics. The following metrics had identified weaknesses.

Metric 1: Continuous Monitoring Management	Metric 2: Configuration Management	Metric 3: Identity and Access Management	Metric 4: Incident Response and Reporting	Metric 5: Risk Management
Metric 6: Security Training	Metric 9: Contingency Planning	Metric 10: Contractor Systems		

Weaknesses in Sections 2, *Configuration Management;* 3, *Identity and Access Management;* 5, *Risk Management*; and 6 *Security Training* resulted in negative conclusions to components of these metrics. For FY 2014, Grant Thornton concluded that the risk and severity of SSA's information security weaknesses were significant enough to constitute a significant deficiency under FISMA.

OIG Evaluation of Grant Thornton's Audit Performance

To fulfill our responsibilities under the *Inspector General Act of 1978*, we monitored Grant Thornton's performance audit of SSA's FY 2014 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.

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

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

Grant Thornton

MEMORANDUM

Date: October 30, 2014

To: SSA Office of the Inspector General

From: Grant Thornton LLP

Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014 – A-14-14-24083

In conjunction with the audit of the Social Security Administration's (SSA) Fiscal Year (FY) 2014 Financial Statements, the Office of the Inspector General engaged us to conduct the performance audit on SSA's compliance with the *Federal Information Security Management Act of 2002* (FISMA) for FY 2014. 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 be and should not be used by anyone other than these specified parties.

Grant Thornton LLP

Alexandria, Virginia
October 30, 2014

Grant Thornton

The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2014 A-14-14-24083

October 2014 **Report Summary**

Objective

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

Background

SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year 2014 FISMA performance audit in accordance with *Government Auditing Standards*, commonly referred to as the "Yellow Book," which sets forth generally accepted government auditing standards. We assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems by leveraging work performed as part of the financial statement audit and through additional testing procedures as needed. We determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and supporting applicable regulations, standards, and guidance applicable during the audit period.

Our Findings

We determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. However, weaknesses in some of the program's components limited the program's effectiveness to adequately protect the Agency's information and information systems. We concluded that these weaknesses constituted a significant deficiency under FISMA.

Our Recommendations

- Implement requirements or appropriately justify deviations associated with the United States Government Configuration Baseline for Windows components.
- Continue, as part of the SSA threat and vulnerability management processes, prioritization and implementation of risk mitigation strategies and plans of action and milestones.
- Develop comprehensive policies and procedures related to application and system-software change management that address issues noted during the audit.
- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.
- Analyze access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and control monitoring.
- 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 requirements are effectively and consistently implemented.
- 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.

SSA agreed with our recommendations.

Grant Thornton

TABLE OF CONTENTS

ABBREVIATIONS

DDS	Disability Determination Services
DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
FISMA	*Federal Information Security Management Act of 2002*
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
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
RO	Regional Office
SA&A	Security Assessment and Authorization
SDLC	System Development Lifecycle
SP	Special Publication
SSA	Social Security Administration
U.S.C.	United States Code
USGCB	United States Government Configuration Baselines

Grant Thornton

OBJECTIVE

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

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

BACKGROUND

In conjunction with the audit of SSA's Fiscal Year (FY) 2014 Financial Statements,[1] SSA's Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the FY 2014 FISMA performance audit. FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002), includes the following key requirements.

- Each agency must develop, document, and implement an agency-wide information security program.[2]
- Each agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.[3]
- The agency's Inspector General (IG), or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.[4]

[1] Office of the Inspector General (OIG) Contract Number GS-23F-8196H, December 3, 2009.

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

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

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

Grant Thornton

SCOPE AND METHODOLOGY

DHS issued 11 reporting metrics, dated December 2, 2013[5] for the IG's FY 2014 FISMA submission. The following DHS reporting metrics were included in the scope of the performance audit:

FY 2014 Inspector General FISMA Reporting Metrics
1. Continuous Monitoring Management
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
11. Security Capital Planning

We conducted the FY 2014 SSA FISMA performance audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, also known as the "Yellow Book." The Yellow Book sets forth generally accepted government auditing standards. 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 2014 Financial Statement Audit (FSA), conducted in accordance with generally 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 the Office of Management and Budget (OMB) and DHS requirements under FISMA to submit an annual report to Congress. Refer to Appendix A for additional information on our scope and methodology.

[5] Metrics posted by DHS on e-Government Community Website.

Grant Thornton

RESULTS OF REVIEW

For FY 2014, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements.[6] However, we identified weaknesses that limited the program's effectiveness to adequately protect the Agency's information and information systems. We concluded that each metric was generally consistent with FISMA requirements, OMB guidance, and applicable National Institute of Standards and Technology (NIST) standards. However, we identified weaknesses in 8 of the 11 metrics. The following metrics had identified weaknesses:

Metric 1: Continuous Monitoring Management	Metric 2: Configuration Management	Metric 3: Identity and Access Management	Metric 4: Incident Response and Reporting	Metric 5: Risk Management
Metric 6: Security Training	Metric 9: Contingency Planning	Metric 10: Contractor Systems		

Refer to Appendix B for additional information on metrics.

Weaknesses in Metric 2, *Configuration Management*, Metric 3, *Identity and Access Management*, Metric 5, *Risk Management*, and Metric 6, *Security Training*, resulted in negative conclusions for the following metrics.

Configuration Management

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

[6] We based our conclusion was based on our assessment of SSA's compliance with DHS' *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*. As indicated in Appendix B, we determined that SSA established all 11 security program components, which were generally consistent with Federal guidance. The 11 components established by SSA included the vast majority of attributes identified by DHS. However, we also noted various issues in our assessment that, which are documented in the comments within Appendix B.

Identity and Access Management

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

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

Risk Management

- Metric 5.1.2 - Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST Special Publication (SP) 800-37, Rev. 1.

Security Training

- Metric 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.

We provided management with comments on these key components of SSA's information security program throughout the audit.[7] Refer to Appendix B for additional information on these and other weaknesses and conclusions.

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

- *USGCB Secure Configuration Settings Deviations* - Documentation for a significant number of Windows deviations from the USGCB settings did not provide sufficient information pertaining to risk analysis and business justification for the deviation. This contributed to the negative conclusion for Metric 2.1.5.

- *Threat and Vulnerability Management* - During our testing of threat and vulnerability management processes we noted issues with network security controls. This contributed to the negative conclusion for Metric 2.1.9 and impacted other metrics in Section 2, *Configuration Management*.

- *Configuration / Change Management* – We noted a lack of comprehensive Agency-wide policy and procedures related to management of application and system-software changes,

[7] 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.

including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results. While this did not contribute to a negative conclusion, metrics within Section 2, *Configuration Management*, were impacted.

- *Mainframe Security* – We noted a lack of controls related to the identification and monitoring of high-risk programs operating on the mainframe.[8] We noted the Agency had not finalized and fully implemented controls associated with ensuring that privileged programs were identified, were approved, could only be modified appropriately, and posed no security risks. While this did not contribute to a negative conclusion, metrics in Section 2, *Configuration Management*, were impacted.

- *Access Controls* - Our testing identified control failures related to appropriate completion of logical access authorization forms and timely removal of location access. Further, we continue to note that SSA did not have an authoritative source to identify and manage all contractors and therefore was unable to supply actual departure dates for contractors to substantiate timely removal of access. Finally, we noted that SSA management continued to make progress in assessing profile[9] content to validate that profiles only provide access to the minimal resources required for users to complete job functions. However, SSA had not completed the review of all profiles that are relevant to critical applications and supporting systems nor had SSA completed other profile quality initiatives including, but not limited to, some control enhancements.

  As a result of these deficiencies, we noted numerous issues of unauthorized and inappropriate access including application developers (programmers) who had unmonitored access to production data and application transactions, key transactions and data, key change management libraries, and other sensitive system software resources. This contributed to the negative conclusion for Metric 3.1.7 and 3.1.10 and impacted other metrics in Section 3, *Identity and Access Management*.

- *IT Oversight and Governance* - During our site visit testing, we noted recurring issues associated with security management, physical access controls, and platform security.[10] Further, we noted areas where the Program Operations Manual System (POMS)[11] guidance was ambiguous or not sufficiently documented, which resulted in inconsistent

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

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

[10] Information system security associated with configurations and privileged access.

[11] POMS is a primary source of information used Social Security employees to process benefit claims for Social Security. It also includes SSA requirements and guidance for implementation of security controls.

implementation or noncompliance with POMS. Finally, we noted that an information system selected for testing, which was developed in a regional office, did not consistently follow SSA's System Development Lifecycle (SDLC) and Security Assessment and Authorization (SA&A) requirements. This contributed to the negative conclusion for Metric 5.1.2 and impacted other metrics in Metric 5, *Risk Management*.

- *Security Training Issues* – Our testing noted that initial, refresher, and specialized security training was not completed or was not completed in a timely fashion for all employees and contractors. Further, we noted that SSA did not have an authoritative system to identify and track the completion of training for all users. This contributed to the negative conclusion for Metric 6.1.4.

For FY 2014, we concluded that the risk and severity of SSA's information security weaknesses, including those listed above, and other weaknesses outlined in Appendix B, were significant enough to constitute a significant deficiency under FISMA[12]. These security deficiencies, when aggregated, created a weakness in SSA's overall information systems security program that we concluded significantly compromised the security of its information and information systems. These weaknesses could impact the confidentiality, integrity, and availability of SSA information systems and data.[13]

Agency Efforts to Resolve Weaknesses and Potential Cause for the FY 2014 FISMA Significant Deficiency

While SSA continued executing its risk based approach to strengthen controls over its systems and address weaknesses, our FY 2014 testing identified similar control issues in both design and operation of key controls. We believe that, in many cases, these deficiencies continue to exist because of one, or a combination, of the following:

- Risk mitigation strategies and related control enhancements require additional time to be fully implemented or to effectuate throughout the environment.

[12] OMB defines a FISMA significant deficiency as, ". . . a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken." OMB, M-14-04, FY 2013 Reporting Instructions for the *Federal Information Security Management Act* and Agency Privacy Management, November 18, 2013, page 8.

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

- 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 to address continuing operational effectiveness issues.

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

CONCLUSIONS AND RECOMMENDATIONS

For FY 2014, we determined that SSA had established an overall information security program and practices that were generally consistent with FISMA requirements. However, weaknesses in some of the program's components limited the program's effectiveness to adequately protect the Agency's information and information systems. We noted weaknesses in Section 2, *Configuration Management*; Section 3, *Identity and Access Management;* Section 5, *Risk Management;* and Section 6, *Security Training,* that resulted in negative answers to metrics and various other issues that resulted in comments to the FISMA metrics in Appendix B. Based on these factors, we concluded that these weaknesses constituted a significant deficiency under FISMA.

SSA needs to protect its mission-critical assets. Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. Some weaknesses identified in this report could cause the Agency's systems and data to lose confidentiality, integrity, and availability to some degree. To mitigate the risks of the issues noted in the significant deficiency, management should consider the following:

- Implement requirements or appropriately justify deviations 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 plans of action and milestones.

- Develop comprehensive policies and procedures related to application and system-software change management that address issues noted during the audit.

- Develop a comprehensive program to identify and monitor high-risk programs operating on the mainframe.

- Analyze access authorization and removal processes to determine whether current controls mitigate the risk of unauthorized access and modify controls considering automation and control monitoring.

- Continue, as part of the SSA profile quality program, additional profile content reviews and profile improvement initiatives.
- Enhance current information technology (IT) oversight and governance processes to ensure SSA IT risk management requirements are effectively and consistently implemented.
- 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. SSA's official responses will be included in their comments to the independent auditor's report on the audit of SSA's FY 2014 financial statements.[14]

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

Grant Thornton

APPENDICES

Grant Thornton

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Management Act of 2002* (FISMA) directs each agency's Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices, as well as a review of an appropriate subset of agency systems.[1] The Social Security Administration's (SSA) IG contracted with us, Grant Thornton LLP (Grant Thornton), to audit SSA's Fiscal Year (FY) 2014 financial statements.[2] Because of the extensive internal control system work that is completed as part of that audit, the FISMA review requirements were incorporated into our financial statement audit (FSA) contract. To maximize efficiencies and minimize the impact to SSA management during the FISMA performance audit, we used Appendix IX – *Application of FISCAM to FISMA* from the GAO *Federal Information System Controls Audit Manual* 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.

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

- FISMA law;
- Office of Management and Budget (OMB) guidance;
- OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Information Resources;
- Standards and guidelines issued by the National Institute of Standards and Technology (NIST) – including, NIST Special Publication (SP) 800-53 Revision 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 (PIV) of Federal Employees and Contractors;*
- OMB Memorandum 15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*;
- Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics; and
- local SSA policies.

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

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

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. These 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.

Grant Thornton

Appendix B – Response to Fiscal Year 2014 Inspector General *Federal Information Security Management Act* Reporting Metrics

Section 1: CONTINUOUS MONITORING MANAGEMENT

1.1. Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

1.1.2. Documented strategy for information security continuous monitoring (ISCM). (AP)

FY2014 Conclusion: Yes

Comments: N/A

1.1.3. Implemented ISCM for information technology assets. (AP)

FY2014 Conclusion: Yes

Comments: N/A

1.1.4. Evaluate risk assessments used to develop their ISCM strategy. (AP)

FY2014 Conclusion: Yes

Comments: We noted that a risk assessment was not completed for one application selected for testing that was developed in a regional office. Therefore, risks associated with this application may not have been considered as part of continuous monitoring processes

1.1.5. Conduct and report on ISCM results in accordance with their ISCM strategy. (AP)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted that the SSA continuous monitoring strategy includes manual control assessments and automated reporting mechanisms. Per the strategy, security controls currently selected for automated continuous monitoring are primarily technical controls that automated support tools can monitor and controls that may change frequently due to architectural or environment modifications as updates and upgrades to hardware or software configurations.

1.1.7. Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). (AP)

FY2014 Conclusion: Yes

Comments: N/A

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

FY 2014 Conclusion: We noted that SSA continued enhancing automated continuous monitoring capabilities in FY 2014. 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

Grant Thornton

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?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

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

2.1.2. Defined standard baseline configurations. (Base)

FY2014 Conclusion: Yes

Comments: We noted that SSA established a list of authorized infrastructure software (platforms), developed baselines for the majority of authorized platforms, and continued to progress in developing additional configuration baselines in FY 2014. However, the Agency had not developed a configuration baseline for one platform selected for testing.

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

FY2014 Conclusion: Yes

Comments: We noted that, while the Agency developed baseline configurations for the majority of authorized platforms, it had not developed a configuration baseline for one platform selected for testing and had not developed procedures to monitor production settings against a baseline for another platform selected for testing. Finally, we noted additional issues during vulnerability assessments.

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

FY2014 Conclusion: Yes

Comments: During our testing of threat and vulnerability management processes, we noted issues with network security controls.

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

FY2014 Conclusion: No

Comments: Documentation for a significant number of Windows (specifically Windows 7 and Vista) deviations from the USGCB settings did not provide sufficient information pertaining to risk analysis and business justification for the deviation.

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

FY2014 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 risk assessments, test plans, and retention of testing output. For application changes, we noted instances where evidence to support testing and other requirements, such as approvals, could not be provided.

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

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

FY2014 Conclusion: Yes

Comments: While we noted that processes were in place for patch management for various platforms selected for testing, the OIG Audit Report A-14-14-14043, *Effectiveness of the Social Security Administration's Server Patch Management Process*, noted that SSA did not have a comprehensive server patch management program.[1]

[1] The OIG report and our testing revealed that patch management processes were in place, however, a comprehensive program was not per the OIG report.

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

FY2014 Conclusion: Yes

Comments: We noted that SSA implemented robust internal and external scanning processes. However, we noted instances where scanning processes could be enhanced.

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

FY2014 Conclusion: No

Comments: During our testing of threat and vulnerability management processes, we noted issues with network security controls.

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

FY2014 Conclusion: Yes

Comments: Refer to 2.1.7.

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.

FY2014 Conclusion: N/A

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted that SSA identified deviations to software through configuration management, patch management, and vulnerability management processes. However, the Agency did not provide sufficient risk analysis and business justification for USGCB Windows deviations, had not developed a robust configuration baseline process for software used in software development projects, and we noted deviations from configuration baselines in our assessment of some platforms selected for testing.

2.3.1. Is there a process for mitigating the risk introduced by those deviations? (Base)

FY2014 Conclusion: Yes

Comments: Refer to comments above.

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?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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 control failures related to the appropriate completion of authorization forms for new hires, transferred employees, and contractors.

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

FY2014 Conclusion: Yes

Comments: We noted that SSA identified when special access requirements were necessary; however, we also noted instances in our testing when these requirements were not followed.

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: No

Comments: 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, key transactions and data, key change management libraries, and other sensitive system software resources.

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

FY2014 Conclusion: Yes

Comments: The OIG Audit Report A-14-13-13050, *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network*, noted that while the Agency had a process to

identify hardware devices connected to its network, we [the OIG] determined the Agency's inventory was incomplete and inaccurate. Additionally, SSA did not approve all of the hardware devices connected to its network. Moreover, although SSA had processes to monitor the security level of connected devices, they were inconsistent with Agency policy in effect at the time of our [the OIG] audit.

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

FY2014 Conclusion: Yes

Comments: We noted that SSA was able to identify user and non-user accounts. However, we noted a lack of requirements to periodically review and change passwords for system accounts and issues associated with the management of vendor accounts.

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

FY2014 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.

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

FY2014 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.

FY2014 Comments: We noted the following:

- A number of employees and contractors gained access to SSA systems before attaining a suitability clearance.

- The OIG Audit Report A-15-13-13092, *Contractor Access to Social Security Administration Data*, noted that SSA did not have a comprehensive, integrated process to identify all of its contractors…We [the OIG] determined that SSA (1) granted systems access to some contractors in excess of what they needed to complete their job functions and (2) did not always terminate contractors' system access timely.

- The OIG Audit Report A-14-14-14051, *Mobile Device Security*, noted that SSA's security of mobile devices did not always conform with Federal standards and business best practices to mitigate unauthorized access to Agency sensitive information. Specifically, we found the Agency lacked a comprehensive, consolidated mobile device policy, did not secure all mobile devices, and provided minimal mobile device security training.

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?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

4.1.3. When applicable, reports to US-CERT within established timeframes (NIST SP 80053, 800- 61; OMB M-07-16, M-06-19). (KFM)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted the incident reporting policy and procedure included information about reporting incidents to appropriate law enforcement groups, including the Office of the Inspector General (OIG), Federal Protective Services (FPS), and local law enforcement. However, it was noted that the policy did not specify the established timeframes in which the various types of incidents should be reported and to whom.

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 M07-16, M-06- 19). (KFM)

FY2014 Conclusion: Yes

Comments: We noted the incident response procedures did not provide guidance nor directives associated with prioritizing incidents, establishing timeframes and/or general guidance in which incidents should be resolved, and escalation processes should incidents not be addressed in a timely fashion. Additionally, we noted that the agency is developing procedures regarding resolving incidents; however, these documents are in draft form.

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

FY2014 Conclusion: Yes

Comments: N/A

4.1.7. Is capable of correlating incidents. (Base)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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.

FY2014 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?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: No

Comments: During our site visit testing, we noted recurring issues associated with security management, physical access controls, and platform security. Further, we noted areas where the Program Operations Manual System (POMS) guidance was ambiguous or not sufficiently documented, which resulted in inconsistent implementation or noncompliance with POMS. Finally, we noted that an information system selected for testing, which was developed in a regional office, did not consistently follow SSA's System Development Lifecycle (SDLC) and Security Assessment and Authorization (SA&A) requirements.

5.1.3. Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 80037, Rev. 1. (Base)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: While we noted that SA&A processes were not consistently followed for a RO application selected for testing, SSA had developed overarching policy and procedures associated with SA&A activities.

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted for an application selected for testing, which was developed in a regional office, that SA&A requirements were not consistently followed, including development of a system security plan (SSP) that identifies and describes the tailored set of baseline security controls.

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

FY2014 Conclusion: Yes

Comments: We noted for an application selected for testing, which was developed in a regional office, that SA&A requirements were not consistently followed, including development of a SSP that identifies and describes the tailored set of baseline security controls. Further, we noted that SSA was in process of implementing control changes based on changes from NIST SP 800-53 revision 3 to revision 4. However, SSA had not documented business justification and/or risk-based determinations for each revision 4 baseline security control that had not been implemented within 1 year since the issuance of the new guidance in April 2013.

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

FY2014 Conclusion: Yes

Comments: We noted for an application selected for testing, which was developed in a regional office, that SA&A requirements were not consistently followed, including assessment of security controls.

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

FY2014 Conclusion: Yes

Comments: We noted for an application selected for testing, that was developed in a regional office, that SA&A requirements were not consistently followed, including completing an authorization to operate (ATO).

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted the following:

- For an application selected for testing, which was developed in a regional office, that SA&A requirements were not consistently followed, including completing an authorization package, including the SSP, security assessment report, and POA&M;
- the SSPs for two applications selected for testing had not been reviewed annually; and,
- the authority to operate (ATO) had expired for one application selected for testing.

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

FY2014 Conclusion: Yes

Comments: We noted for an application selected for testing, which was developed in a regional office, that SA&A requirements were not consistently followed, including completing a security authorization package.

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.

FY2014 Comments: N/A

Grant Thornton

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?

FY2014 Conclusion: Yes

6.1.1. Documented policies and procedures for security awareness training (NIST SP 80053: AT- 1). (Base)

FY2014 Conclusion: Yes

Comments: We noted that the SSA security awareness training policy did not include a timeframe for the completion of initial security awareness training upon becoming employed with SSA.

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

FY2014 Conclusion: Yes

Comments: We noted that specialized training procedures did not specify or provide guidance on the type of training required based on the user's significant information security responsibilities. As such, training for some selected employees and contractors did not correspond to the user's responsibilities and/or security.

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

FY2014 Conclusion: Yes

Comments: We noted that specialized training procedures did not specify or provide guidance on the type of training required based on the user's significant information security responsibilities. As such, training for selected users did not correspond to the user's responsibilities and/or security.

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)

FY2014 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.

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)

FY2014 Conclusion: Yes

Comments: We noted that specialized training policy and procedures did not specify or provide guidance on the type of training required based on the user's significant information security responsibilities. As such, training for selected employees and contractors with significant security responsibilities did not correspond to the user's responsibilities and/or security. Additionally, while SSA requires 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)

FY2014 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?

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

7.1.8. Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04- 25). (Base)

FY2014 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.

FY2014 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?

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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.

FY2014 Comments: N/A

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

FY2014 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?

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted that SSA documented recovery time objectives within the enterprise operational assurance assessment and business continuity considerations within continuity of operations plans (COOP). However, SSA did not consistently consider and document business impact analysis based on newly developed applications and significant changes to existing applications. Therefore, impacts to overall recovery objectives and business processes may not effectuate to those charged with recovery responsibilities for systems or business functions.

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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)

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 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.

FY2014 Comments: N/A

Section 10: CONTRACTOR SYSTEMS

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

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

10.1.2. The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2). (Base)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted that a system listed on SSA's information system inventory was not appropriately labeled as a contractor system.

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

FY2014 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)

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: We noted that before a contractor system was implemented, SSA SA&A processes were not completed, including the ATO CISO Recommendation Letter, the ATO decision letter, and a comprehensive business continuity plan.

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.

FY2014 Comments: N/A

Section 11: SECURITY CAPITAL PLANNING

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

FY2014 Conclusion: Yes

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Conclusion: Yes

Comments: N/A

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

FY2014 Comments: N/A

Grant Thornton

Appendix C – The Social Security Administration's General Support Systems and Major Applications

	System	Acronym
	General Support Systems[1]	
1	Audit Trail System	ATS
2	Comprehensive Integrity Review Process	CIRP
3	Death Alert Control and Update System	DACUS
4	Debt Management System	DMS
5	Enterprise Wide Mainframe & Distributed Network Telecommunications Services 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 Applications[2]	
1	Electronic Disability System	eDib
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR
5	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Social Security Number Establishment and Correction System	SSNECS
8	Title II	T2

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

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

Grant Thornton

Appendix D – METRICS DEFINED

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

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

- **Identify and Access Management -** Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files.

- **Incident Response and Reporting -** According to the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage.

- **Risk Management –** Risk Management is "[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.

- **Security Capital Planning –** According to OMB M-14-04, "Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(C)) A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes."

Appendix E – MAJOR CONTRIBUTORS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Managing Director, Grant Thornton

Cal Bassford, Senior Manager, Grant Thornton

Chris Malarkey, Manager, Grant Thornton

Olga Mason, Senior Associate, Grant Thornton

Jessica Saunders, Senior Associate, Grant Thornton

MISSION

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

CONNECT WITH US

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

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

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


Watch us on YouTube


Like us on Facebook


Follow us on Twitter


Subscribe to our RSS feeds or email updates

OBTAIN COPIES OF AUDIT REPORTS

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

REPORT FRAUD, WASTE, AND ABUSE

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

Website:	http://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing