

Audit Report

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



**Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION**

MEMORANDUM

Date: November 26, 2013

Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013 (A-14-13-13086)

The attached final report summarizes Grant Thornton, LLP's, (Grant Thornton) Fiscal Year (FY) 2013 audit of the Social Security Administration's (SSA) information security program and practices, as required by Title III of the *E-Government Act of 2002*, Public Law Number 107-347. Title III is also known as the *Federal Information Security Management Act of 2002* (FISMA).

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

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

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

Objective, Scope, and Methodology

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

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

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

Audit Results

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

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

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

OIG Evaluation of Grant Thornton's Audit Performance

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

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

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

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

A handwritten signature in black ink, appearing to read "Patrick P. O'Carroll, Jr."

Patrick P. O'Carroll, Jr.

Attachment



MEMORANDUM

Date: November 26, 2013

To: SSA Office of the Inspector General

From: Grant Thornton, LLP

Subject: The Social Security Administration's Compliance with the Federal Information Security Management Act of 2002 for Fiscal Year 2013 (A-14-13-13086)

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

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

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

Alexandria, Virginia
November 26, 2013

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

November 2013

Report Summary

Objective

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

Background

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

Our Findings

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

Our Recommendations

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

TABLE OF CONTENTS

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

ABBREVIATIONS

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

OBJECTIVE

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

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

BACKGROUND

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

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

SCOPE AND METHODOLOGY

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

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

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

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

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

FY 2013 Inspector General FISMA Reporting Metrics

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

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

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

RESULTS OF REVIEW

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

⁵ Our conclusion was based on our assessment of SSA’s compliance with DHS’ *FY 2013 Inspector General Federal Information Security Management Act Reporting Metrics*. As indicated in Appendix B, we determined that SSA established all 11 security program components, which were generally consistent with Federal guidance. The 11 components established by SSA included the vast majority of attributes identified by DHS. However, we also noted various issues in our assessment that are documented in the comments within Appendix B.

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

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

Refer to Appendix D for additional information on metrics.

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

Configuration Management

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

Identity and Access Management

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

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

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

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

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

- *Lack of comprehensive Agency-wide policy and procedures related to management of application and system software changes, including identification of all critical types of changes, security categorization and risk analysis for changes, testing requirements based on risk, and requirements for the review and approval of testing results* – While our testing demonstrated that change management activities were occurring for application and system software changes, the Agency had not fully documented a comprehensive policy and procedures covering the entirety of the change management processes conducted by the Agency. Our testing noted the following.

- System Software - An impact/risk assessment to determine the security implications for mainframe changes did not occur. Further, for the majority of changes tested, we noted that developers were responsible for testing their own changes and implementing these changes into production. While management performed a review to validate that updates made were associated with an approved change, there were no requirements nor guidance related to the types of testing to be performed (including security reviews), nor for retention or

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

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

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

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

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

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

- *Access control issues* - Our testing identified numerous issues with logical access controls that are in place to mitigate the risk of unauthorized access. Our testing identified the following issues:

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

⁷ International Business Machines Corp. defines a mainframe as computers that can support thousands of applications and input/output devices to simultaneously serve thousands of users. A mainframe is the central data repository, or hub, in a corporation's data processing center, linked to users through less powerful devices such as workstations or terminals.

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

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

For FY 2013, we concluded that the risk and severity of SSA's information security weaknesses, including those highlighted above and other weaknesses outlined in Appendix B, were great enough to constitute a **significant deficiency** under FISMA. These weaknesses could result in losses of confidentiality, integrity, and availability of SSA information systems and data.⁹

OMB defines a FISMA significant deficiency as, "... a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."¹⁰

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

⁸ A profile is one of SSA's primary access control mechanisms. Each profile contains a unique mix of facilities and transactions that determines what access to systems resources a specific position needs.

⁹ **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. **Integrity** means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. **Availability** means ensuring timely and reliable access to and use of information. Pub. L. No. 107-347, Title III, Section 301 § 3542(b)(1)(A) to (C), 44 U.S.C. § 3542(b)(1)(A) to (C).

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

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

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

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

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

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

CONCLUSIONS AND RECOMMENDATIONS

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

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

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

SSA needs to protect its mission-critical assets. Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. Some weaknesses identified in this report could cause the Agency's systems and data to lose confidentiality, integrity, and availability to some degree.

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

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

VIEWS OF RESPONSIBLE OFFICIALS

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

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

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

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

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

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

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

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

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

Our assessment followed the DHS FY 2013 FISMA guidance³ and focused on Risk Management, Configuration Management, Incident Response and Reporting, Security Training, Plan of Action and Milestones, Remote Access Management, Identity and Access Management, Continuous Monitoring Management, Contingency Planning, Contractor Systems, and Security Capital Planning.

We conducted this audit in accordance with generally accepted government auditing standards. These standards required that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on the audit objectives.

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

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

Section 1: CONTINUOUS MONITORING MANAGEMENT

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

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

FY2013 Conclusion: Yes

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

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

Comments: N/A

Section 2: CONFIGURATION MANAGEMENT

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

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

2.1.2. Defined standard baseline configurations. (Base)

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

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

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

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

FY2013 Conclusion: No

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

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

FY2013 Conclusion: No

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

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

FY2013 Conclusion: Yes

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

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: No

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

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

FY2013 Conclusion: No

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

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

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

FY2013 Conclusion: Yes

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

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

Comments: N/A

Section 3: IDENTITY AND ACCESS MANAGEMENT

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: No

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: No

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

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

FY2013 Conclusion: Yes

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

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

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

Comments: N/A

Section 4: INCIDENT RESPONSE AND REPORTING

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

4.1.7. Is capable of correlating incidents. (Base)

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

Section 5: RISK MANAGEMENT

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

Section 6: SECURITY TRAINING

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A



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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

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

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

Section 8: REMOTE ACCESS MANAGEMENT

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

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

FY 2013 Conclusion: Yes

Comments: N/A

Section 9: CONTINGENCY PLANNING

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

Section 10: CONTRACTOR SYSTEMS

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

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

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

Section 11: SECURITY CAPITAL PLANNING

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

FY2013 Conclusion: Yes

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

FY2013 Conclusion: Yes

Comments: N/A

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

Comments: N/A

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

	System	Acronym
General Support Systems¹		
1	Audit Trail System	ATS
2	Comprehensive Integrity Review Process	CIRP
3	Death Alert Control and Update System	DACUS
4	Debt Management System	DMS
5	Enterprise Wide Mainframe & Distributed Network Telecommunications Services and System	EWANS
6	FALCON Data Entry System	FALCON
7	Human Resources Management Information System	HRMIS
8	Integrated Client Database System	ICDB
9	Integrated Disability Management System	IDMS
10	Quality System	QA
11	Security Management Access Control System	SMACS
12	Social Security Online Accounting & Reporting System	SSOARS
13	Social Security Unified Measurement System	SUMS
Major Applications²		
1	Electronic Disability System	eDib
2	Earnings Record Maintenance System	ERMS
3	National Investigative Case Management System	NICMS
4	Recovery of Overpayments, Accounting and Reporting System	ROAR
5	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
6	Supplemental Security Income Record Maintenance System	SSIRMS
7	Social Security Number Establishment and Correction System	SSNECS
8	Title II	T2

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

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

Appendix D – METRICS DEFINED

- **Continuous Monitoring Management** - Continuous Monitoring maintains ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
- **Configuration Management** - From a security point of view, Configuration Management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications.
- **Identify and Access Management** - Identity and Access Management includes policies to control user access to information system objects, including devices, programs, and files.
- **Incident Response and Reporting** - According to the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-12, the two main benefits of an incident-handling capability are (1) containing and repairing damage from incidents and (2) preventing future damage.
- **Risk Management** – “Risk Management is the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.”
NIST Special Publication 800-53, Rev. 3, page B-11.
- **Security Training** - According to FISMA, Title III of the *E-Government Act of 2002* (Pub. L. No. 107-347, December 17, 2002) an agency wide information security program for a Federal agency must include security awareness training. This training must cover (1) information security risks associated with users’ activities and (2) users’ responsibilities in complying with agency policies and procedures designed to reduce these risks.
- **Plan of Action and Milestones (POA&M)** – According to OMB M-14-04, “Plan of Action and Milestone (POA&M) (defined in OMB Memorandum M-02-01), A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.”
- **Remote Access Management** - Refers to controls associated with remote access to the information systems from virtually any remote location.

- **Contingency Planning** - Processes and controls to mitigate risks associated with interruptions (losing capacity to process, retrieve, and protect electronically maintained information) that may result in lost or incorrectly processed data.
- **Contractor Systems** - Agencies are responsible for ensuring that appropriate security controls are in place over contractor systems used or operated by contractors or other entities (such as other Federal or state agencies) on behalf of an agency.
- **Security Capital Planning** – According to OMB M-14-04, “Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(C)) A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.”

Appendix E – MAJOR CONTRIBUTORS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Electronic Data Processing Partner, Grant Thornton

Cal Bassford, Director, Grant Thornton

Jessica Saunders, Senior Associate, Grant Thornton

Olga Mason, Senior Associate, Grant Thornton

Kevin Potter, Associate, Grant Thornton

MISSION

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

CONNECT WITH US

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

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

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



[Watch us on YouTube](#)



[Like us on Facebook](#)



[Follow us on Twitter](#)



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

OBTAIN COPIES OF AUDIT REPORTS

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

REPORT FRAUD, WASTE, AND ABUSE

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

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

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

FAX: 410-597-0118

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

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