OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

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

A-14-16-50037 | November 2015

OIG Office *of the* Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date:	November 12, 2015	Refer To:	
To:	The Commissioner		
From:	Inspector General		
Subject:	The Social Security Administration's Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015 (A-14-16-50037)		

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

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

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

Objective, Scope, and Methodology

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

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

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

Grant Thornton's Audit Results

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

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

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

OIG Comments

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

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

> . . . a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the

> agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.[2]

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

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

OIG Evaluation of Grant Thornton's Audit Performance

To fulfill our responsibilities under the *Inspector General Act of 1978*, we monitored Grant Thornton's performance audit of SSA's FY 2015 compliance with FISMA by

- reviewing Grant Thornton's audit approach and planning;
- evaluating its auditors' qualifications and independence;
- monitoring the audit progress;
- examining Grant Thornton's working papers;
- reviewing Grant Thornton's audit report to ensure it complies with government auditing standards;
- coordinating the issuance of the audit report; and
- performing other procedures as deemed necessary.

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

Grant Thornton is responsible for the attached auditor’s report and the opinions and conclusions expressed therein. The OIG is responsible for technical and administrative oversight regarding Grant Thornton performance under the terms of the contract. Our review, as differentiated from an audit in accordance with applicable auditing standards, was not intended to enable us to express, and, accordingly, we do not express, an opinion about the effectiveness of SSA’s information security policies, procedures, and practices. However, our monitoring review, as qualified above, disclosed no instances where Grant Thornton did not comply with applicable auditing standards.

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

Patrick P. O’Carroll, Jr.

Attachment

Grant Thornton

MEMORANDUM

Date: November 12, 2015 **Refer To:**

To: SSA Office of the Inspector General

From: Grant Thornton

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

In conjunction with the audit of the Social Security Administration’s (SSA) Fiscal Year (FY) 2015 Financial Statements, the Office of the Inspector General engaged us to conduct the performance audit on SSA’s compliance with the *Federal Information Security Modernization Act of 2014* (FISMA) for FY 2015. The objective was to determine whether SSA’s overall information security program and practices were effective and consistent with FISMA requirements, as defined by the Department of Homeland Security. We are pleased to report the results of our audit and appreciate the support provided to us in completing this review.

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

Grant Thornton LLP

Alexandria, Virginia
October 30, 2015

Grant Thornton

The Social Security Administration’s Compliance with the Federal Information Security Modernization Act of 2014 for Fiscal Year 2015
A-14-16-50037

November 2015 **Report Summary**

Objective

Our objective was to determine whether the Social Security Administration’s (SSA) overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), as defined by the Department of Homeland Security (DHS).

Background

SSA’s Office of the Inspector General (OIG) engaged us, Grant Thornton LLP (Grant Thornton), to conduct the Fiscal Year (FY) 2015 FISMA performance audit in accordance with Government Auditing Standards. We assessed the effectiveness of SSA’s information security controls including its policies, procedures, and practices on a representative subset of the Agency’s information systems by leveraging work performed as part of the financial statement audit and by performing additional testing procedures as needed. We used the DHS OIG FY 2015 Inspector General (IG) FISMA reporting metrics as the basis for our assessment of SSA’s overall information security program and practices.

Findings

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

Recommendations

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

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

TABLE OF CONTENTS

ABBREVIATIONS

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

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

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), as defined by the Department of Homeland Security (DHS).[1] To achieve this objective, we assessed the effectiveness of SSA's information security policies, procedures, and practices on a representative subset of the Agency's information systems. We then determined whether SSA's overall information security program and practices were effective and consistent with the requirements of FISMA and other regulations, standards, and guidance applicable during the audit period.

BACKGROUND

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

- Each agency must develop, document, and implement an agency-wide information security program.[3]
- Each agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems.[4]
- The agency's Inspector General (IG), or an independent external auditor, must perform an independent evaluation of the agency's information security program and practices to determine their effectiveness.[5]

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

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

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

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

[4] Pub. L. No. 1137-283, § 2 § 3554(a)(1)(A); 44 U.S.C. § 3554(a)(1)(A).

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

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

Scope and Methodology

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

FY 2015 Inspector General FISMA Reporting Metrics	
1.	Continuous Monitoring Management[7]
2.	Configuration Management
3.	Identity and Access Management
4.	Incident Response and Reporting
5.	Risk Management
6.	Security Training
7.	Plan of Action & Milestones (POA&M)
8.	Remote Access Management
9.	Contingency Planning
10.	Contractor Systems

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

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

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

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

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

RESULTS OF REVIEW

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

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

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

[9] **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. **Integrity** means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. **Availability** means ensuring timely and reliable access to and use of information. Pub. L. No. 113-283, § 2, §§ 3552(b)(3)(A) to (C), 44 U.S.C. §§ 3552(b)(3)(A) to (C).\

[10] OMB, M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013, page 8. To date, OMB's definition of significant deficiency remains the same. OMB's *Fiscal Year (FY) 2015 Frequently Asked Questions on Reporting for the Federal Information security Management Act and Agency Privacy Management*, page 15, provides the OMB's significant deficiency definition, https://community.max.gov/x/eQPENw.

Significant Information Security Control Weaknesses

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

Configuration Management

- SSA's documentation did not provide sufficient risk analysis, justification, and approval for a significant number of deviations from United States Government Configuration Baseline (USGCB) secure configuration settings.

- We identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner, as specified in organization policy or standards.[12]

Identity and Access Management

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

- We identified control failures related to the timely removal of terminated employees' logical access to the mainframe, network, and other supporting systems.

- SSA did not have an authoritative source to identify departure dates for individual contractors; therefore, the Agency was unable to supply actual departure dates for contractors to substantiate timely removal of their systems access.

Risk Management

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

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

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

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

- We noted SSA had not applied its RMF across all decentralized systems; as such, not all information systems had formal system security plans (SSP) or were mapped to an existing boundary with an SSP. Therefore, appropriately tailored sets of baseline security controls were not determined (or identified) and documented across all systems. In addition, we noted inconsistencies with documentation and implementation of common controls, hybrid controls, and system specific controls based on our reviews of entity level SSPs and information system specific SSPs.

- We noted that, without appropriately selected and documented sets of controls and assessments, the security controls may not be implemented as intended. Further, without consistency in mapping of common, hybrid, and system-specific controls, implementation of such controls may not be appropriate.

- SSA had not applied its RMF requirements across all decentralized systems. Consequently, security controls may not be appropriately assessed, and information systems may be in operation without an authorization to operate (ATO).

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

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

Security Training

- SSA did not have an authoritative system to identify and track completion of security awareness training for all employees and contractors.

- We noted numerous instances where evidence was not available to substantiate the completion of training for employees and contractors.

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

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

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

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

CONCLUSIONS AND RECOMMENDATIONS

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

SSA needs to protect its mission-critical assets. Without appropriate security, the Agency's systems and the sensitive data they contain are at risk. Some weaknesses we identified could negatively impact the confidentiality, integrity, and availability of the Agency's systems and data. We believe that SSA must strengthen its information security risk management framework and enhance information technology oversight and governance to address these weaknesses.

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

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

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

VIEWS OF RESPONSIBLE OFFICIALS

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

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

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

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

- Assessed the risk associated with these applications as low because regional applications are smaller in scope and do not process programmatic or financial transactions. They are not tied to financial systems. Almost 300 of these “applications” are region-specific tools that do not contain personal information, e.g., spreadsheets or static SharePoint sites. Due to the lack of financial impact or significance, we consider these applications lower risk. There are existing regional oversight processes to manage risk in these applications until we develop the standardized SA&A process.

- Extended our mature and robust process for assessing the security of our mission-critical systems to include our decentralized applications. The newly developed SA&A process for regionally developed applications, includes assigning the 600+ applications to security authorization boundaries as well as documenting and assessing the security controls in place. We plan to fully implement this process by Q1 of FY16. We developed this process for managing security risks in a comprehensive and consistent manner for applications developed in our regions.

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

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

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

- The findings that Grant Thornton cites as recurring are minor documentation issues; examples include references to incomplete checklists and references to code documentation for a system that is 30 years old. Following best practices and to make the best use of limited resources, we take a risk based approach to addressing findings and we consider these types of documentation findings to be low risk issues. We prioritized our FY2015 improvements to address issues identified as higher risk. We will continue to standardize and improve our documentation.

- In FY 2015 we implemented the electronic form-120 to improve access control to SSA systems resources and by Q1 FY16, will implement the Security Access Management (SAM) workflow tool which will further improve the control of access to systems resources.

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

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

GRANT THORNTON RESPONSE

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

- Regarding vulnerability management, while areas of improvement were identified, testing continued to reveal weaknesses. As noted in metric 2.1.8, our information security and penetration testing, vulnerability management, and configuration management assessments identified control weaknesses with cyber/network security controls, many of which continue to exist from past audits.

- Regarding the risk management results, as SSA indicated, our conclusions for many metrics in FY 2015 were cited as a "no" compared to a "yes" in FY 2014. We expanded our scope in FY 2015 based on findings from our prior year report to include additional testing of a second region and we performed additional inquiry to assess SSA's implementation of risk management activities throughout the regions and the DDS sites. In our discussions with SSA we learned that the DDS case processing systems and potentially over 600 regional office applications had not been subjected to risk management activities, i.e. SA&A. Further, during the audit period, SSA was still in the process of completing SA&A activities for the two regional applications selected for testing. The results from our increased scope revealed

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

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

- Regarding the risk associated with the applications, SSA stated that a risk assessment was completed and the regional applications were determined to be low risk. However, FISMA requirements extend beyond financial and mission-critical systems; security requirements should be implemented across an organization. Information system weaknesses, even in lower risk applications and supporting systems, can lead to exposures that may impact financial or mission-critical data and/or result in data loss. Further, these findings extend to disability case processing systems that are hosted at DDS locations. These systems play a significant role in benefit processing for disability claims and should be considered major applications.

- Regarding the DDS sites, SSA had not fully implemented the standardized security plan during our audit period and we continued to identify platform security concerns across the DDS sites visited in FY 2015. DCPS was also not applicable to the current audit period.

- Regarding the recurring issues identified in our field work, we believe these are indicative of a lack of oversight and governance. Numerous issues continue to persist from past audits and minimal corrective action had been taken through the audit period to address the findings. For example, platform security issues for the DDS sites have been reported in management letter comments to the Agency dating back to 2004. Further, in response to SSA's comments on recurring issues:

    - Security Management – Issues cited in the current year included weaknesses in performance of background checks and a lack of comprehensive and approved system security plans. In addition, we continued to note areas where SSA's security requirements/guidance to DDSs was ambiguous, inconsistent, or not sufficiently documented. An appropriate security management program and system security plans afford management the opportunity to provide appropriate direction and oversight of the design, development, and operation of critical system controls. Lack of appropriate controls may result in inconsistent implementation and application of security measures.

    - Physical and Logical Access – Issues cited in the current year included weaknesses in performance of physical access recertification, inappropriate physical access to sensitive areas, terminated individuals retaining physical access to sensitive areas, as well as, logical access, and issues with logical access authorization. The electronic form-120 did not reduce the types of issues identified in past years and SAM was not implemented during the audit period.

  - Platform Security – SSA discussed its security risk configuration standards and scans for the DDS systems. However, our testing continued to identify weaknesses in the platform security of decentralized sites tested. In regards to the DDSs, we identified weaknesses in reviewing compliance against SSA's risk configuration standards, configurations on the platforms not aligned with SSA's standards, a lack of reviews over inactive accounts, a lack of evidence to support reviews of users with privileged access, instances of inappropriate access to sensitive accounts, and instances of weak credentials. Finally, we noted issues associated with vendor account management and audit logging/monitoring.

- Regarding cloud systems, our assessment focused on information systems that SSA stated met its definition of cloud computing models (please note SSA adopted the NIST definition of cloud computing models). For systems we tested, SSA had not met FedRAMP requirements, contrary to the Agency's documented policy/procedures. Specifically, SSA requirements stated, "SSA will only use FedRAMP evaluated and compliant cloud service providers (CSP). If the cloud system is not FedRAMP compliant and was built by an external private sector CSP, the agency should inform the CSP that the system is not FedRAMP compliant, and advise the CSP that FedRAMP requirements should have been met by June 5, 2014."

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

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

The *Federal Information Security Modernization Act of 2014* (FISMA) directs each agency's Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices, as well as a review of an appropriate subset of agency systems.[1] The objective of Grant Thornton LLP's (Grant Thornton) audit was to determine whether the Social Security Administration's (SSA) overall information security program and practices were effective and consistent with the FISMA requirements, as defined by the Department of Homeland Security (DHS). Annually, DHS publishes reporting metrics to be utilized as the basis for this assessment. SSA's IG contracted with us, Grant Thornton, to audit SSA's Fiscal Year (FY) 2015 financial statements and perform the FY 2015 FISMA performance audit. Because of the extensive internal control system work that is completed as part of that audit, the FISMA review requirements were incorporated into our financial statement audit (FSA) contract. To maximize efficiencies and minimize the impact to SSA management during the FISMA performance audit, we used Appendix IX – *Application of FISCAM to FISMA from the GAO Federal Information System Controls Audit Manual* to leverage testing performed during the SSA FSA. In some cases, FISMA tests were unique from those of the FSA; therefore, we designed test procedures to deliver adequate coverage over those unique areas. We assessed information systems internal controls, as they were significant to the audit objectives and DHS IG reporting metrics, using Federal Information System Controls Audit Manual guidance including performance of inquiry, observation, and inspection procedures.

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

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

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

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

- Standards and guidelines issued by the National Institute of Standards and Technology (NIST) – including, NIST Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations*; Federal Information Processing Standards Publication (FIPS) - 199, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS-200 *Minimum Security Requirements for Federal Information and Information Systems*, FIPS- 201-1, *Personal Identity Verification of Federal Employees and Contractors;* and other NIST publications cited in DHS' annual FISMA IG reporting metrics;

- Other Federal guidance and standards cited in the DHS annual FISMA IG reporting metrics; and,

- Applicable SSA policies.

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

Appendix B – Response to Fiscal Year 2015 Inspector General *Federal Information Security Modernization Act* Reporting Metrics

Section 1: CONTINUOUS MONITORING MANAGEMENT

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

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

Level 2 - Defined

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

Level 2 - Defined

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

Level 2 – Defined

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

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

Level 2 – Defined

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

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

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

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

Section 2: CONFIGURATION MANAGEMENT

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

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

2.1.2. Defined standard baseline configurations. (Base)

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: No

Comments: During our testing of threat and vulnerability management processes, we identified weaknesses in network security controls, which indicated that SSA did not always remediate configuration-related vulnerabilities, including scan findings, in a timely manner, as specified in organization policy or standards. Specific disclosure of detailed information about these weaknesses might further compromise controls and are therefore not provided within this report. Rather, the specific details are presented in a separate, limited-distribution management letter.

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

FY 2015 Conclusion: Yes

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

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

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: Refer to comments for 2.3.

Section 3: IDENTITY AND ACCESS MANAGEMENT

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: No

Comments: We identified numerous issues with logical access controls including adequate completion of approval forms for new and transferred information system users, recertification processes, and with the timely removal of logical access which may have contributed to instances of inappropriate and/or unauthorized access identified as part of testing. This includes, but may not be limited to, application developers (programmers) with unmonitored access to production and application transactions, as well as, other users with inappropriate access to data, change management libraries, and other privileged functions/sensitive system software resources.

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

Comments: We noted the following:

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

Section 4: INCIDENT RESPONSE AND REPORTING

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

4.1.6. Is capable of correlating incidents. (Base)

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Comments: N/A

Section 5: RISK MANAGEMENT

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: No

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

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

FY 2015 Comments: N/A

Section 6: SECURITY TRAINING

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: No

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

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

Comments: N/A

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

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Comments: N/A

Section 8: REMOTE ACCESS MANAGEMENT

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

Section 9: CONTINGENCY PLANNING

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Comments: N/A

Section 10: CONTRACTOR SYSTEMS

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

FY 2015 Conclusion: Yes

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: We noted that SSA generally identified contractor systems, but did not consistently obtain assurance that security controls and FISMA requirements were effectively implemented for contractor systems selected for testing. Specifically, we noted instances of incomplete or missing SSPs, Authority to Operate (ATO) letters, and Business Continuity Plan (BCP).

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

FY 2015 Conclusion: Yes

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

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Conclusion: Yes

Comments: N/A

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

FY 2015 Comments: N/A

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

	System	Acronym
	General Support 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	Retirement, Survivors, Disability Insurance Accounting System	RSDI ACCTNG
5	Supplemental Security Income Record Maintenance System	SSIRMS
6	Social Security Number Establishment and Correction System	SSNECS
7	Title II	T2

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

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

Appendix D– METRICS DEFINED

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

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

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

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

- **Risk Management** – Risk Management is "[t]he program and supporting process to manage risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time." NIST Special Publication 800-53, Rev. 4, page B-11.19.

- **Security Training** - According to FISMA, Title III of the E-Government Act of 2002 (Pub. L. No. 107-347, December 17, 2002) an agency-wide information security program for a Federal agency must include security awareness training. This training must cover (1) information security risks associated with users' activities and (2) users' responsibilities in complying with agency policies and procedures designed to reduce these risks.

- **Plan of Action and Milestones (POA&M)** – According to OMB M-14-04, "Plan of Action and Milestone (POA&M) (defined in OMB Memorandum M-02-01), a POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems."

- **Remote Access Management** - Refers to controls associated with remote access to the information systems from virtually any remote location.

- **Contingency Planning** - Processes and controls to mitigate risks associated with interruptions (losing capacity to process, retrieve, and protect electronically maintained information) that may result in lost or incorrectly processed data.

- **Contractor Systems** - Agencies are responsible for ensuring that appropriate security controls are in place over contractor systems used or operated by contractors or other entities (such as other Federal or state agencies) on behalf of an agency.

Appendix E – ACKNOWLEDGMENTS

Eveka Rodriguez, Engagement Partner, Grant Thornton

Greg Wallig, Principal, Grant Thornton

Cal Bassford, Senior Manager, Grant Thornton

Olga Mason, Manager, Grant Thornton

John O’Brien, Manager, Grant Thornton

Jessica Saunders, Manager, Grant Thornton

Kirsten Orr, Senior Associate, Grant Thornton

Kevin Potter, Senior Associate, Grant Thornton

Mitali Surti, Senior Associate, Grant Thornton

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