

**Office of Inspector General
Corporation for National and
Community Service**

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

INDEPENDENT EVALUATION FOR FY 2013

OIG REPORT 14-03

Office of Inspector General

Corporation for
**NATIONAL &
COMMUNITY
SERVICE** 

1201 New York Ave, NW
Suite 830
Washington, DC 20525

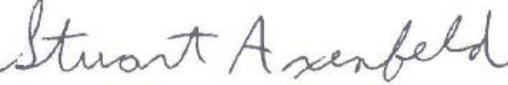
(202) 606-9390

This report was issued to Corporation management on December 16, 2013. Under the laws and regulations governing audit follow-up, the Corporation is to make final management decisions on the report's findings and recommendations no later than June 16, 2014, and complete its corrective actions by December 15, 2014. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.



December 16, 2013

TO: Kim Mansaray
Chief Operating Officer (Acting)

FROM: Stuart Axenfeld 
Assistant Inspector General Audit

SUBJECT: Federal Information Security Management Act (FISMA)
Independent Evaluation for FY 2013 (OIG Report Number 14-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 14-03 "FY13 Federal Information Security Management Act (FISMA) Evaluation for the Corporation for National and Community Service." This evaluation was performed by Kearney & Company, P.C. in accordance with the Quality Standards for Inspection and Evaluation promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE).

Kearney & Company, P.C. has determined that the Corporation has limited assurance that its Information Security Program is compliant with the FISMA legislation, applicable Office of Management and Budget (OMB) guidance, and National Institute of Standards and Technology (NIST) Special Publications (SP). Their evaluation identified 30 instances of noncompliance with OMB guidance and NIST SPs. These areas of noncompliance are grouped into six findings, resulting in nine recommendations to strengthen the Corporation's Information Security Program.

Should you have any questions about this report, please contact Guy Hadsall, Chief Technology Officer/OIG at 202-606-9375.

Attachment

cc:
Philip Clark, Chief Information Officer
Lloyd Samples, Chief Information Security Officer



**FY 2013 Federal Information Security
Management Act Evaluation**

for the

**Corporation for National and Community
Service**

RQ#: OIG1302130001, Amendment CNSIG-13-Q-0002

December 13, 2013



Point of Contact:
Tyler Harding, Principal
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
tyler.harding@kearneyco.com

Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

TABLE OF CONTENTS

	<u>Page #</u>
1. BACKGROUND	3
1.1 Overview	3
1.2 FISMA.....	3
1.3 NIST Security Standards and Guidelines.....	4
1.4 DHS’s FISMA Responsibilities	5
1.5 Scope	6
2. SUMMARY RESULTS.....	6
3. FINDINGS.....	8
3.1 ISCM Strategy.....	8
3.2 Risk Management.....	11
3.3 Security Awareness and Training	15
3.4 Evaluation of Agency POA&M Process	18
3.5 Evaluation of Contractor Oversight	19
3.6 Identity and Access Management Controls.....	22
APPENDIX A: MANAGEMENT’S RESPONSE.....	25
APPENDIX B: KEARNEY’S AND OIG’S ANALYSIS OF PLANNED ACTIONS.....	37
APPENDIX C: RESULTS FROM NCCC AND STATE FIELD OFFICE ASSESSMENTS.....	53
APPENDIX D: ABBREVIATIONS AND ACRONYMS.....	54
APPENDIX E: REFERENCED DOCUMENTS	55

December 13, 2013

Honorable Deborah J. Jeffrey
Inspector General
Office of Inspector General
Corporation for National and Community Service
1201 New York Avenue, NW, Suite 830
Washington, D.C. 20525

Dear Ms. Jeffrey:

This report presents the results of Kearney & Company, P.C.'s (defined as "Kearney," "we," and "our" in this report) independent evaluation of the Corporation for National and Community Service's (the Corporation) Information Security Program and practices. The Federal Information Security Management Act of 2002 (FISMA) requires the Corporation to develop, document, and implement an agency-wide Information Security Program to protect its information and information systems, including those provided or managed by another agency, contractor, or source. Additionally, FISMA requires the Corporation to undergo an annual independent evaluation of its Information Security Program and practices, as well as an assessment of its compliance with FISMA requirements. The Corporation's Office of Inspector General (OIG) contracted with Kearney to perform an independent fiscal year (FY) 2013 FISMA evaluation of the Corporation's information technology (IT) policies, procedures, and practices. We are pleased to provide this FY 2013 FISMA Independent Evaluation Report, which details the results of our review of the Corporation's Information Security Program.

The objectives of the evaluation were to:

- Determine the efficiency and effectiveness of the Corporation's IT policies, procedures, and practices
- Review a representative subset of the Corporation's information systems
- Assess the Corporation's compliance with FISMA and related information security policies, procedures, standards, and guidelines
- Evaluate personally identifiable information (PII) protection and physical controls at field office sites
- Prepare the Corporation's responses to the Department of Homeland Security's (DHS) *FY 2013 Inspector General (IG) FISMA Reporting Metrics*, dated November 30, 2012.

Kearney's methodology for the FY 2013 FISMA evaluation included testing a subset of the Corporation's systems for compliance with selected controls covered by the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision (Rev.) 3, *Recommended Security Controls for Federal Information Systems and Organizations*. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation*, promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE), and included

inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

The Corporation's Information Security Program incorporates security requirements required by FISMA, and updates them as guidance changes. For example, the Corporation is currently transitioning from NIST SP 800-53, Rev. 3 to NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to increase assurance that security controls have been adequately implemented and assessed. The Corporation is also continuing to update its information security policies and procedures; oversee its primary technology contractor, SRA International, Inc. (SRA), and other contracted services; and provide training in proper protection of PII for field office personnel.

We conclude that the Corporation has limited assurance that its Information Security Program is compliant with the FISMA legislation, applicable Office of Management and Budget (OMB) guidance, and NIST SPs. Our testing identified 30 instances of noncompliance with OMB guidance and NIST SPs, itemized in Appendix C: *Responses to DHS's FY 2013 IG FISMA Reporting Metrics*. These areas of noncompliance are grouped into six findings, and our report includes nine recommendations to strengthen the Corporation's Information Security Program. Appendix A provides the Corporation's response to the draft FISMA report.

In closing, we appreciate the courtesies extended to the Kearney FISMA Evaluation Team during this engagement.

Sincerely,

A handwritten signature in blue ink that reads "Kearney & Company". The signature is written in a cursive, flowing style.

Kearney & Company, P.C.
Alexandria, Virginia

1. BACKGROUND

1.1 Overview

In 1993, the Corporation was established to connect Americans of all ages and backgrounds with opportunities to give back to their communities and their nation. Its mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. The Corporation's Board of Directors and Chief Executive Officer (CEO) are appointed by the President and confirmed by the Senate. The CEO oversees the agency, which employs about 600 employees operating throughout the United States and its territories. The Board of Directors sets broad policies and direction for the Corporation, and oversees actions taken by the CEO with respect to standards, policies, procedures, programs, and initiatives, as are necessary to carry out the mission of the Corporation.

1.2 FISMA

FISMA was enacted into law as Title III of the E-Government Act of 2002 (E-Gov) (Public Law [P.L.] 107-347, December 17, 2002). Key requirements of FISMA include:

- The establishment of an agency-wide Information Security Program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source
- An annual independent evaluation of the agency's Information Security Program and practices
- Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.

FISMA outlines the information security management requirements for agencies, including the requirement for an annual review and independent assessment by each agency's IG. The statute also requires minimum standards for agency systems. The annual assessments are intended to assist agencies in developing strategies and best practices for improving information security.

In addition, FISMA requires Federal agencies to implement the following information security practices:

- Periodic risk assessments
- Information security policies, procedures, standards, and guidelines
- Delegation of authority to the Chief Information Officer (CIO) to ensure the design and implementation of information security policies are consistent with OMB and NIST guidance
- Security awareness training programs
- Periodic testing and evaluation of the effectiveness of security policies, procedures, and practices, to be performed no less than annually
- Processes to manage remedial actions for addressing deficiencies
- Procedures for detecting, reporting, and responding to security incidents

- Plans to ensure continuity of operations
- Annual reporting on the adequacy and effectiveness of the Information Security Program to OMB and Congress.

OMB is responsible for reporting to Congress a summary of the results of an agency's compliance with FISMA requirements. OMB also establishes executive policies with respect to information security. Its principal written statement of Government policy regarding information security is OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, dated November 28, 2000, which establishes a minimum set of controls to be included in Federal automated Information Security Programs. In particular, OMB Circular A-130, Appendix III defines adequate security as security commensurate with the risk and magnitude of the harm resulting from loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Additionally, OMB has issued guidance related to information security with regard to Plans of Actions and Milestones (POA&M) for addressing findings from security control assessments, security impact analyses, and continuous monitoring activities. Per OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*, POA&Ms provide a roadmap for ensuring continuous agency security improvement, and assisting agency officials with prioritizing corrective action and resource allocation.

1.3 NIST Security Standards and Guidelines

FISMA requires NIST to establish minimum standards and guidelines for Federal information systems, and further requires Federal agencies to comply with Federal Information Processing Standards (FIPS) issued by NIST. These requirements cannot be waived. NIST also develops and issues SPs as recommendations and guidance documents.

FIPS Publication (PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates the use of NIST SP 800-53, Rev. 3¹, *Recommended Security Controls for Federal Information Systems and Organizations*. NIST SP 800-53, Rev. 3 provides guidelines for selecting and specifying security controls for information systems. The security controls described in NIST SP 800-53 are organized into 18 functional "families" that fall into three broad classes—technical, management, and operational²—shown in Table 1 below.

¹ NIST released its fourth revision of the SP on April 30, 2013.

² According to NIST SP 800-53, management controls are the security controls for an information system that focus on the management of risk and information system security. Operational controls are the security controls for an information system that are primarily implemented and executed by people (as opposed to systems). Technical controls are the security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Table 1: Security Control Families

#	Security Control Family	Control Class
1	Access Control	Technical
2	Audit and Accountability	Technical
3	Identification and Authentication	Technical
4	System and Communications Protection	Technical
5	Security Assessment and Authorization	Management
6	Planning	Management
7	Risk Assessment	Management
8	System and Services Acquisition	Management
9	Program Management	Management
10	Awareness and Training	Operational
11	Configuration Management	Operational
12	Contingency Planning	Operational
13	Incident Response	Operational
14	Maintenance	Operational
15	Media Protection	Operational
16	Physical and Environmental Protection	Operational
17	Personnel Security	Operational
18	System and Information Integrity	Operational

Information systems are further categorized according to their importance to the agency’s mission and the potential impact on the agency’s operations, assets, or individuals of a loss of confidentiality, integrity, and availability of the information system and data (see FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*). Of the Corporation’s 10 information systems and sub-systems, six have a “moderate” security impact and four have a “low” security impact. Nine of the 10 information systems are hosted and operated by other Government agencies or third party service providers.

1.4 DHS’s FISMA Responsibilities

Under the authority of OMB, DHS facilitates the annual reporting of the CIO Reporting Metrics, Senior Agency Official for Privacy Reporting Metrics, and OIG Reporting Metrics to Congress, utilizing an online tool called CyberScope. For OIGs to prepare their annual responses in CyberScope, DHS provides instructions in the *FY 2013 IG FISMA Reporting Metrics*, and requires each agency OIG to respond to 11 FISMA metric questions. Appendix B contains the OIG’s responses for the Corporation.

Kearney’s evaluation of the effectiveness of the Corporation’s Information Security Program focused on compliance with FISMA legislative requirements, applicable OMB and NIST guidance, and the Corporation’s own information security policies, procedures, and practices.

1.5 Scope

This independent evaluation was conducted during the period of June through October 2013. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation*, promulgated by CIGIE, including inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls. The FISMA evaluation included an assessment of the following:

- Corporation Information Security Program activities
- Management oversight of contractor-managed systems, including the Corporation Network and My AmeriCorps Portal
- FY 2013 OMB/DHS Reporting Metrics
- Site visits to a Corporation State Office in Jackson, MS
- Site visits to two National Civilian Community Corps (NCCC) locations (Perry Point, MD and Vicksburg, MS).

2. SUMMARY RESULTS

This section provides the conclusions of our research, analysis, and assessment of the Corporation’s Information Security Program, policies, and practices. Authoritative policies, standards, and guidance are cited where applicable. As shown in Table 2 below, Kearney concluded that management attention is needed for seven of the 11 areas of security controls.

Table 2: Security Control Effectiveness

2013 DHS IG FISMA Reporting Area	Security Control Effectiveness
1. Continuous Monitoring Management	Warrants Management Attention
2. Configuration Management	Demonstrates Effectiveness
3. Identity and Access Management	Warrants Management Attention
4. Incident Response and Reporting	Demonstrates Effectiveness
5. Risk Management	Warrants Management Attention
6. Security Training	Warrants Management Attention
7. POA&Ms	Warrants Management Attention
8. Remote Access Management	Warrants Management Attention
9. Contingency Planning	Warrants Management Attention
10. Contractor Systems	Demonstrates Effectiveness
11. Security Capital Planning	Demonstrates Effectiveness

In some of these areas, the Corporation was actively working to address noted security weaknesses and documenting planned activities in POA&Ms. Where the Corporation was making sufficient progress, we did not report a separate finding; instead, we listed those areas in Table 2 above and in Appendix B. Thus, our report focuses on significant unaddressed security control deficiencies grouped into six findings, as listed below in order of significance:

1. Lack of a formally documented and fully implemented Information Security Continuous Monitoring (ISCM) strategy

2. Lack of formally documented and fully implemented Risk Management Framework (RMF)
3. Lack of a fully implemented a Role-Based Information Security Training Program
4. Improvements needed with POA&M reporting
5. Improvements needed to ensure that contractors comply with the Corporation's Information Security Program requirements
6. Lack of two-factor authentication to the Corporation's desktops, laptops, and corporate network.

Addressing these security control deficiencies will assist the Corporation's ongoing efforts to assure adequate security over its information resources. Our report includes nine recommendations to further strengthen the Corporation's Information Security Program. At the time of our evaluation, the Corporation had already taken steps toward strengthening controls in some of these areas:

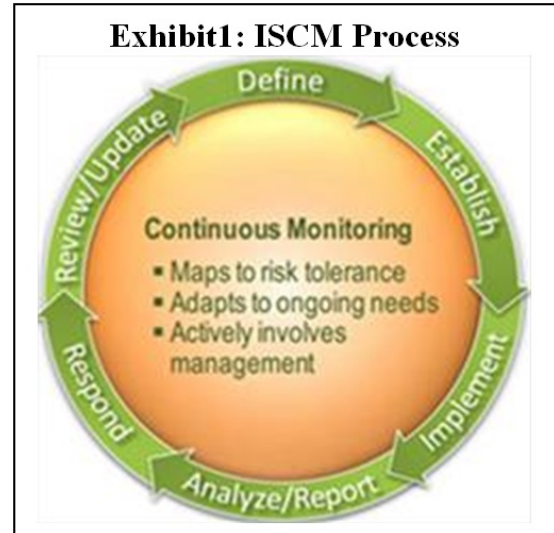
1. Document and fully implement an ISCM strategy
2. Document and fully implement a process for addressing risk at the organizational/mission and business process levels throughout the organization
3. Clearly assign ownership and responsibilities for executing risk management processes at the business/program level (Tier 2)
4. Ensure compliance with processes for monitoring security controls at the information system level, and obtain formal approval and necessary waivers for departures from corporate policy. Further, establish and communicate potential disciplinary actions for noncompliance with the Corporation's security policies
5. Implement role-based security training for all users with significant information security responsibilities and maintain documentation for the completion of training
6. Enhance the POA&M reporting/review process to include details of resources required for remediation, and an explanation for any delays in implementing corrective actions
7. Strengthen the POA&M process to require individuals to reference evidence supporting the closure of a POA&M item
8. Strengthen contractor oversight to ensure compliance with the Corporation's security requirements by clearly assigning oversight responsibility and required activities for Contracting Officers (CO), system owners, and supporting IT professionals
9. Research avenues to implement two-factor authentication, such as leveraging Federal shared service providers to reduce upfront technology costs, lower per unit cost, and adopt a gradual, phased-deployment strategy to overcome current budget constraints.

3. FINDINGS

3.1 ISCM Strategy

Background:

Information Security Continuous Monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. According to NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, effective ISCM begins with development of a strategy that addresses ISCM requirements and activities at each organizational tier (i.e., organization, mission/business process, and information system). Each tier monitors security metrics and assesses security control effectiveness with established monitoring and assessment frequencies, and status reports customized to support tier-specific decision-making. NIST describes continuous monitoring as a six step process, as depicted in Exhibit 1: ISCM Process.



Finding #1: Lack of a Formally Documented and Fully Implemented ISCM Strategy
(See Appendix B, related DHS Question #1: Continuous Monitoring Management)

Condition:

The Corporation has not formally documented and implemented an organization-wide ISCM strategy, as mandated by OMB guidance and required by four NIST SPs. The Corporation’s Information Assurance Program (IAP) provides for the continuous monitoring of information system (Tier 3) controls; however, the IAP does not define all processes supporting a continuous monitoring program across the entire organization or define meaningful, reportable metrics for all business processes supporting the Corporation’s mission.

An ISCM strategy consists of activities at three levels within an organization: Tier 1 – Organization, Tier 2 – Mission/Business Process, and Tier 3 – Information System. Such activities should include the following:

1. Policy that defines key metrics
2. Policy for modifications to and maintenance of the monitoring strategy
3. Policies and procedures for the assessment of security control effectiveness (common, hybrid, and system-level controls)
4. Policies and procedures for security status monitoring
5. Policies and procedures for security status reporting (on control effectiveness and status monitoring)
6. Policies and procedures for assessing risks, and gaining threat information and insights
7. Policies and procedures for configuration management and security impact analysis

8. Policies and procedures for implementation and use of organization-wide tools
9. Policies and procedures for establishment of monitoring frequencies
10. Policies and procedures for determining sample sizes and populations, and managing object sampling
11. Procedures for determining security metrics and data sources
12. Templates for assessing risks
13. Templates for security status reporting (on control effectiveness and status monitoring).³

Cause:

The Corporation is currently in the process of revising procedural documentation and has not fully adopted the current guidance from NIST regarding continuous monitoring. According to the Corporation's CIO, the Corporation has a strategy for continuous monitoring; this strategy is reflected in the Corporation's daily security practices. With a small team of security professionals, the CIO thought that the strategy was adequately communicated without documentation. Additionally, the impact of sequestration resulted in an approximate 12% IT budget decrease and left fewer resources available for implementing information security initiatives.

Criteria:

In 2009, OMB and NIST acknowledged that the then-existing Government-wide approach of re-assessing all general support systems and major applications every three years, as required by OMB Circular A-130, Appendix III, did not address the dynamic nature of IT and the constantly changing threat landscape to the organization, business/mission, and supporting information systems. OMB and NIST therefore determined that agencies needed to develop near-real time continuous monitoring practices. OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, provides specific guidance regarding continuous monitoring and risk management practices. OMB states in its Frequently Asked Questions:

29: Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130? No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to conduct ongoing authorizations of information systems through the implementation of continuous monitoring programs. Continuous monitoring programs thus fulfill the three-year security reauthorization requirement, so a separate re-authorization process is not necessary. In an effort to implement a more dynamic, risk-based security authorization process, agencies should follow the guidance in NIST Special Publication 800-37. Agencies should develop and implement continuous monitoring strategies for all information systems which address all security controls implemented, including the frequency and degree of rigor associated with the monitoring process. Continuous monitoring strategies should also include all common controls inherited by organizational information systems. Continuous monitoring strategies should be developed in accordance with NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, and

³ NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, Section 3.1, "Define ISCM Strategy."

approved by appropriate authorizing officials. Agency officials should monitor the security state of their information systems on an ongoing basis with a frequency sufficient to make ongoing risk-based decisions on whether to continue to operate the systems within their organizations. Continuous monitoring programs and strategies should address: (i) establishment of metrics to be monitored; (ii) establishment of frequencies for monitoring/assessments; (iii) ongoing security control assessments to determine the effectiveness of deployed security controls; (iv) ongoing security status monitoring; (v) correlation and analysis of security-related information generated by assessments and monitoring; (vi) response actions to address the results of the analysis; and (vii) reporting the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.

NIST provides specific guidance to Federal agencies for implementing a continuous monitoring program in four key NIST SPs, listed below in order of precedence:

- NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009. Please refer to required Security Control CA-7, “Continuous Monitoring”; and related Security Controls RA-2, “Security Categorization”; CA-2, “Security Assessment”; and CA-6, “Security Authorization”
- NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010. This SP discusses the NIST RMF, which comprises six steps that provide a structured practice for incorporating information security and risk management activities into the system development lifecycle
- NIST SP 800-39, *Managing Information Security Risk*, March 2011. This SP provides guidelines for developing an ISCM strategy and implementing an ISCM program
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. This SP describes the fundamentals of ongoing monitoring in support of risk management.

Effect:

Failure to implement a comprehensive ISCM strategy weakens of the internal control environment and increases the risk that inappropriate or unusual activity could go undetected, possibly allowing fraud or unauthorized transactions. The Corporation is working to mitigate this risk by adopting more recent NIST guidance and practices; however, these practices were not fully implemented during FY 2013.

The bottom line is that the lack of a comprehensive and documented strategy leaves the Corporation with important gaps in its IT security monitoring, such as its oversight of contractor operated information systems. An ISCM strategy is a critical first step in identifying and rectifying these and other gaps and ensuring that sensitive systems and information are secure.

Recommendation:

Kearney recommends that the Corporation:

1. Document and fully implement an ISCM strategy that incorporates the following:
 - a. Establishment of metrics to be monitored
 - b. Establishment of frequencies for monitoring/assessments
 - c. Ongoing security control assessments to determine the effectiveness of deployed security controls
 - d. Ongoing security status monitoring
 - e. Correlation and analysis of security-related information generated by assessments and monitoring
 - f. Response actions to address the results of the analysis
 - g. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.

3.2 Risk Management

Background:

Title III of the E-Gov, entitled FISMA, emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

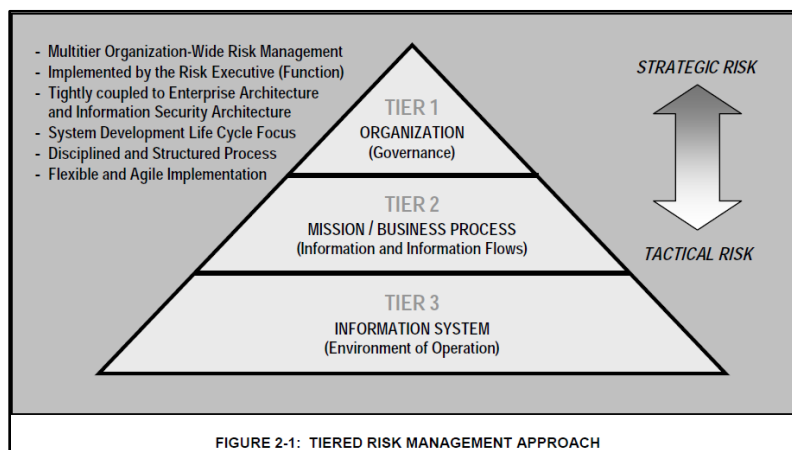
Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision, and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the “front lines” operating the information systems supporting the organization’s missions/business functions. NIST defines the key elements for effectively managing information security risk organization-wide as follows:

- Assignment of risk management responsibilities to senior leaders/executives
- Ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the nation arising from the operation and use of information systems
- Establishing the organizational tolerance for risk and communicating that risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities
- Accountability by senior leaders/executives for their risk management decisions, and for the implementation of effective, organization-wide risk management programs
- Understanding the organizational missions and business functions, and the relationships among missions/business functions and supporting processes.

In an era of constrained budgets, Federal agencies are increasingly integrating and consolidating various internal control and risk management activities to reduce duplication of effort. To gain efficiencies, several Federal agencies are centralizing responsibilities for conducting OMB Circular A-123 internal control assessments along with required FISMA risk management and security assessment activities under a central program office for internal controls. In another

example, a Federal agency reorganized management responsibilities to make a single Chief Security Officer responsible for information security, physical security, personnel security (i.e., background checks), and risk management activities. These examples reflect how different agencies are addressing multiple OMB mandates for stronger internal controls and improved risk management practices.

Risk management can be viewed as a “holistic” activity that is fully integrated into every aspect of the organization. NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, Section 2.1, “Integrated Organization-Wide Risk Management,” illustrates a three-tiered approach to risk management that addresses risk-related concerns at the organization level, the mission and business process level, and the information system level.



Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy that includes the following:

- Techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization
- Methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment
- Types and extent of risk mitigation measures the organization plans to employ to address identified risks
- Level of risk the organization plans to accept (i.e., risk tolerance)
- How the organization plans to monitor risk on an ongoing basis, given the inevitable changes to organizational information systems and their environments of operation
- Degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

Tier 2 addresses risk from a mission and business process perspective, and is guided by the risk decisions at Tier 1. Tier 2 activities are closely associated with enterprise architecture and include the following:

- Defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations)
- Prioritizing missions and business processes with respect to the goals and objectives of the organization
- Defining the types of information that the organization needs to successfully execute the stated missions and business processes, and the information flows both internal and external to the organization
- Developing an organization-wide information protection strategy and incorporating high-level information security requirements into the core missions and business processes
- Specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Tier 3 addresses risk from an information system perspective and is guided by the risk decisions at Tiers 1 and 2. Tier 3 risk management activities include the following:

- Categorizing organizational information systems
- Allocating security controls to organizational information systems and the environments in which those systems operate consistent with the organization's established enterprise architecture and embedded information security architecture
- Managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development lifecycle process implemented across the organization.

Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST SP 800-53.

Finding #2: Lack of Formally Documented and Fully Implemented RMF

(See Appendix B, related DHS Question #5: Risk Management)

Condition:

The Corporation's risk management program addresses risk mainly at the information system (Tier 3) level. Policy and documented processes for system-level assessments were substantially compliant with requirements; however, Kearney noted the following:

- The Corporation lacks an organization-wide risk assessment that considers risks across the organization, including Tier 2 activities/business processes carried out by field offices
- The Corporation did not annually assess the security controls or risks of its Electronic System for Programs, Agreements, and National Service (eSPAN) application.

Cause:

The Corporation has not yet completed revisions to its information security procedures to comply with the current guidance from NIST. Additionally, the impact of sequestration resulted in an approximate 12% IT budget decrease and left fewer resources available for implementing information security initiatives. Further, discussions with the Corporation's CIO⁴/Risk Executive expressed the view that, as a "small agency," the Corporation does not need to adopt and/or document formal risk management strategies, as these decisions are reflected in corporate security policies. The CIO/Risk Executive also commented that the distinction between internal controls and information security controls at the business/program level (Tier 2) are unclear. Lacking this clarity, the CIO/Risk Executive indicated that ultimate responsibility and ownership of risk at the business/program level was not well defined; thus, risk management activities focused on the business/program level did not occur.

Additionally, the Corporation's risk management program does not have a mature process for addressing risk from an organizational perspective, or an established process for monitoring selected security controls for information systems. Specific to the eSPAN observation and lack of a recent security assessment, management indicated that the eSPAN application was being upgraded over several years and delayed a comprehensive security assessment until the upgrade was complete to minimize security assessment costs. Such an approach, while perhaps cost-effective, does not comply with OMB Memoranda and NIST security guidance.

Criteria:

NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, states:

Tier 1 addresses risk from an *organizational* perspective by establishing and implementing *governance* structures that are consistent with the strategic goals and objectives of organizations and the requirements defined by federal laws, directives, policies, regulations, standards, and missions/business functions. Governance structures provide oversight for the risk management activities conducted by organizations and include: (i) the establishment and implementation of a *risk executive (function)*; (ii) the establishment of the organization's risk management strategy including the determination of *risk tolerance*; and (iii) the development and execution of organization-wide *investment strategies* for information resources and information security. *governance* is the set of responsibilities and practices exercised by those responsible for an organization (e.g., the board of directors and executive management in a corporation, the head of a federal agency) with the express goal of: (i) providing strategic direction; (ii) ensuring that organizational mission and business objectives are achieved; (iii) ascertaining that risks are managed appropriately; and (iv) verifying that the organization's resources are used responsibly.

Tier 2 addresses risk from a *mission* and *business process* perspective and is guided by the risk decisions at **Tier 1**. The risk management activities at Tier 2 begin with the identification and establishment of *risk-aware mission/business processes* to support the

⁴ The Corporation's CIO also holds the role of Risk Executive, as defined in NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*.

organizational missions and business functions. Implementing risk-aware mission/business processes requires a thorough understanding of the organizational missions and business functions and the relationships among missions/business functions and supporting processes. **Tier 2** activities are closely associated with enterprise architecture and include: (i) defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations); (ii) prioritizing missions and business processes with respect to the goals and objectives of the organization; (iii) defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization; (iv) developing an organization-wide information protection strategy and incorporating high-level information security requirements¹⁸ into the core missions and business processes; and (v) specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Effect:

An incomplete or out-of-date risk management program could leave the Corporation's management unaware of information security risks affecting the organization and its systems. Without this knowledge, management may not take sufficient actions to reduce risk to the Corporation's programs.

Recommendations:

Kearney recommends that the Corporation:

2. Document and fully implement a process for addressing and capturing risk at the organizational/mission and business process levels throughout the organization
3. Clearly assign ownership and responsibilities for executing risk management processes at the business/program level (Tier 2)
4. Ensure compliance with processes for monitoring security controls at the information system level (i.e., Tier 3), and obtain formal approval and necessary waivers for departures from Corporation policy. Further, establish and communicate potential disciplinary actions for noncompliance with the Corporation's security policies.

3.3 Security Awareness and Training

Background:

Worldwide, some of the most effective attacks on cyber networks currently are directed at exploiting user behavior. As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. These threats are especially effective when directed at those with elevated network privileges and/or other cyber responsibilities. Training users (privileged and unprivileged) and those with access to other pertinent information and media is a necessary deterrent to these methods. Therefore, organizations are expected to use risk-based analysis to determine the correct amount, content, and frequency of updates to achieve adequate security in the area of influencing these behaviors that affect cyber security.

FISMA not only requires organizations to ensure all users of information and information systems are aware of their information security responsibilities (Security Awareness and Training Program), but also requires departments and agencies to identify and train those users with significant responsibilities for information security (Role-based Training). Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today’s highly networked systems environment without ensuring that all people involved in using and managing IT:

- Understand their roles and responsibilities related to the organization’s mission
- Understand the organization’s IT security policies, procedures, and practices
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

Finding #3: Lack of a Fully Implemented of a Role-based Information Security Training Program

(See Appendix B, related DHS Question #6: Security Training)

Condition:

Although the FISMA legislation, OMB, and NIST require role-based security training for individuals with significant information security responsibilities, the Corporation has not documented and implemented a comprehensive role-based security program. Certain role-based security training modules have been developed, but have not yet been approved and disseminated throughout the Corporation.

Cause:

The role-based security training module has been developed by IT staff, but has not been formally approved and deployed throughout the Corporation. The Information Assurance Team stated that budget constraints and emergency IT priorities have contributed to the delay. The Corporation expects role-based security training to be implemented in December 2013. The Corporation’s CIO also indicated that Corporation provides one-on-one training to individuals with significant information security responsibility when they assume a new role; however, the Corporation does not maintain evidence of this training.

Criteria:

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, cites that a successful IT security program consists of:

1. Developing IT security policy that reflects business needs tempered by known risks
2. Informing users of their IT security responsibilities, as documented in agency security policies and procedures
3. Establishing processes for monitoring and reviewing the program.

NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Section AT-3, “Security Training,” states:

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization’s information security program.

The Corporation’s *Information Assurance Program*, Section 3.2, “IA Awareness & Training,” includes the following requirements:

Table 3: Security Training Requirements

Type	Objective	Frequency	Training Provider	Required Participation
Program-Level Training				
Security Training	Promote understanding of information security and privacy policies	1) Annually 2) When changes are made to policies	CISO	All
Security Awareness	Basic understanding of how to respond to risk	1) Annually	CISO	All
Security Role-Based Training	Carry out information assurance risk management roles at the program level	1) Initial training 2) Annually	CISO	Individuals with Program-Level Security Roles
System Specific-Level Training				
System Specific Security Training	Understanding of system specific security and privacy procedures (e.g., Rules of Behavior)	1) Initial training (before access to systems or information) 2) When changes are made to procedures 3) Annually	ISO	All
Security Role-Based Training	Provides security-related training specifically tailored for their assigned duties at the system level (e.g., incident response training)	1) Initial training (before performing duties) 2) Policy is changed 3) Annually	ISO	Individuals with Security Roles

Effect:

A strong IT security program cannot be implemented without significant attention given to training agency IT users on security policies, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. Failure to give attention to security training puts an enterprise at great risk because security of agency resources is as much a human issue as it is a technology issue. Without specific training, a user may not know all of his/her information security responsibilities under the Corporation's policies and may be more vulnerable to cyber-attacks. Additionally, without regular training, individuals with significant information security responsibilities may not keep abreast of new OMB and NIST guidance.

Recommendation:

Kearney recommends that the Corporation:

5. Implement role-based security training for all users with significant information security responsibilities and maintain documentation for the completion of training.

3.4 Evaluation of Agency POA&M Process

Background:

OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*, requires agencies to identify and report on deficiencies in their Information Security Program. A POA&M is a tool that identifies tasks that need to be accomplished. It details the required resources, milestones towards meeting the task, and scheduled completion dates for the milestones. The purpose of this 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.

Finding #4: Improvements Needed to POA&M Reporting

(See Appendix B, related DHS Question #7: Plan of Actions and Milestones)

Condition:

Kearney identified the following procedural weaknesses with the Corporation's management of POA&Ms:

- POA&Ms did not clearly identify resources (labor hours and/or costs) required to resolve open tasks
- Supporting evidence for closing open POA&Ms was not consistently referenced and maintained in the Corporation's POA&M tracker.

Cause:

The Corporation's CIO indicated that when security weaknesses are identified and POA&Ms created, the Corporation opens a Change Request. The Corporation utilizes the Change Request to track priorities and resources necessary for closing the POA&M item. The Corporation's prior POA&M process did not record the associated Change Request number with the POA&M

item. Additionally, the POA&M closure process did not require the participants to maintain evidence of closure.

Criteria:

According to OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*:

POA&Ms should contain, at minimum, (i) the stated weakness, (ii) the point of contact for the POA&M, (iii) the resources required to complete the POA&M, (iv) the scheduled date of completion, (v) the identified milestones complete with anticipated dates of completion, (vi) changes to the milestones, (vii) the source of the weakness, and (viii) the status of the POA&M. POA&Ms not only create a way to track and remediate weaknesses, but can be a valuable tool to communicate resource needs to Agency leadership and should be integrated with the annual budget process when significant investments are required.

Effect:

Without clearly identifying resources needed to plan for and remediate identified security weaknesses, the Corporation may not adequately budget and identify resources required to remediate identified vulnerabilities. Further, POA&M closures may not be adequately supported and reviewed, resulting in potential vulnerabilities.

Recommendations:

Kearney recommends that the Corporation:

6. Enhance the POA&M process to identify resources required for remediation either in the POA&M item or associated change request ticket
7. Strengthen the POA&M process to require individuals to reference evidence supporting the closure of a POA&M item.

3.5 Evaluation of Contractor Oversight

Background:

FISMA and OMB policy require external providers handling Federal information or operating information systems on behalf of the Federal Government to meet the security requirements applicable to Federal agencies. Requirements for external providers, which include security controls for processing, storing, or transmitting Federal information, must be expressed in contracts or similar formal agreements. Organizations can require external providers to implement all steps in the RMF, with the exception of the security authorization step. A Federal agency that chooses to outsource IT services remains ultimately responsible for ensuring appropriate security.

FISMA also requires Federal agencies to provide appropriate protection of their resources through implementing a comprehensive Information Security Program that is commensurate with the sensitivity of the information being processed, transmitted, and stored by agency information

systems. An institutionalized information security performance measurement program enables agencies to collect and report on relevant FISMA performance indicators.

Finding #5: Improvements Needed to Ensure that Contractors Comply with the Corporation’s Information Security Program Requirements

(See Appendix B, related DHS Question #10: Contractor Systems)

Condition:

Although the Corporation has defined general responsibilities for its COs, system owners, and IT support professionals to monitor its IT contractors, the Corporation does not have systems or processes in place to ensure that its employees actually provide the necessary oversight to confirm that contractors implement mandated security controls. Corporation guidance expressly requires the Corporation to ensure contractors, grantees, and other parties that operate information systems for the Corporation or handle data on the Corporation’s behalf adhere to FISMA, OMB requirements, and the Corporation’s information security and privacy policies. Table 4 on the following page summarizes the applicable oversight responsibilities, as detailed by the previous Corporation’s Chief Information Security Officer (CISO).

Table 4: Oversight Procedures Summary

OVERSIGHT PROCEDURES SUMMARY TABLE			
Task	Primary Responsibility	Supporting Roles	Task Completion or Report Date
IT Inventory Registration	Information System Owner, Information Owner, or the individual initiating the procurement of the IT service	Project/Program Manager, Service Provider	Prior to Implementation
FISMA Language/Memorandum of Understanding	Information System Owner, Information Owner, or the individual initiating the procurement of the IT service	Project/Program Manager	Development of the Service Agreement
Preliminary Privacy Impact Assessments	Information System Owner, Information Owner, or the individual initiating the procurement of the IT service	Project/Program Manager, Service Provider	Prior to Collecting Information
Certification and Accreditation	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	Prior to System Activation
Update System Security Plan	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	April 15 th (Annually)
Continuous Monitoring	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	April 15 th (Annually)
Contingency Plan Testing	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	April 15 th (Annually)
Security and Awareness Training	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	April 15 th (Annually)
POA&M	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	As Required
Privacy/Security Incidents	Information System Owner, Information Owner, or Project/ Program Manager	Service Provider	Upon Discovery or Detection

After reviewing IT contracts for the Corporation's Managed Data Center Services (MDCS) provider (SRA), its data center provider (Savvis), and support services contracts for the eSPAN/MyAmeriCorps portal (enGenius and Planned Systems International), together with the procedures setting forth the relevant oversight activities, Kearney determined that the Corporation's process does not describe in sufficient detail the steps and evaluation criteria necessary for review of security assessment documentation (i.e., updated System Security Plan, Continuous Monitoring Plan, Contingency Plan test results, or updated POA&M) and security performance measures required from its IT contractors. Further, the IT contracts appeared to use a generic list of security requirements, but did not specify the security controls or a tailored set of security controls relevant to those contracted IT services. In addition, the IT contracts did not define information security goals and objectives, performance measures, and technical compliance requirements for measuring performance effectiveness, efficiency, or frequency of control execution.

Cause:

The Corporation's management acknowledged that the Corporation was not following the oversight procedures described by its own documentation, in part because the procedures were not communicated to Corporation personnel charged with responsibility. Further, while the use of a generic list of security requirements may have been intended to promote consistency and shift the burden of compliance to the contractor, it was confusing and counterproductive because neither the Corporation nor contractor personnel understood clearly which of the 240+ NIST security controls, Corporation-specific requirements, and policies were relevant to each service contract; how oversight would be implemented; and how contractor compliance would be measured. The Corporation's management also expressed the view that they conducted oversight of its IT contractors and their security controls throughout the year, but did not consistently maintain evidence of this oversight for all IT contracts and conduct it according to the due dates listed in Table 4 above.

Criteria:

NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, Section SA-9, "External Information System Services," states:

Control: The organization:

- a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;
- b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and
- c. Monitors security control compliance by external service providers.

NIST SP 800-35, *Guide to Information Technology Security Services*, dated October 2003, states:

4.5.1 Monitor Service Provider Performance:

The operational phase is similar to the assessment phase. The data collected during the assessment phase should be used to capture the performance level of this new service provider. During the operations phase, the desired future arrangement becomes the current arrangement.

The targets set forth in the service agreement should be compared with the metrics gathered. Although metrics will provide service-level targets, the organization may also want to use end user evaluations or customer satisfaction level surveys to evaluate performance. The IT security managers will have to work with other operational managers (such as customer service managers) to ensure that the service provider is meeting service targets. The IT security managers also need to ensure service providers are complying with IT security policy and processes, as well as applicable laws and regulations. IT security managers must ensure during the operations phase that the service provider does not compromise private, confidential, personal, or mission-sensitive data. Compliance reports will help with this effort. The service agreement should have included clauses that specify penalties and/or remedies for noncompliance and management should employ these when the service provider does not perform as the contract dictates.

Effect:

Without formal monitoring processes and clearly assigned responsibilities for monitoring contractor performance, weaknesses in the security controls implemented by the Corporation's contractors may not be detected, potentially resulting in significant errors and irregularities. This may place the Corporation's data at risk.

Recommendation:

Kearney recommends that the Corporation:

8. Strengthen contractor oversight to ensure compliance with the Corporation's security requirements by clearly assigning oversight responsibility and required activities for COs, system owners, and supporting IT professionals.

3.6 Identity and Access Management Controls

Background:

The key goal of identity and access management is to limit access to those individuals or processes that require use of otherwise restricted information. Identity and access management controls work together to affirm the logical identity of a user, process, or application, and appropriately control access to computer resources (e.g., data, equipment, facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Identity controls are

implemented using authentication factors such as an account ID, password, physical token, fingerprint, or Personal Identity Verification (PIV) card.

Given the rise in sophisticated malware that steals account IDs and passwords, OMB and DHS have mandated that Federal agencies strengthen identity and access management controls to thwart such attacks by using multi-factor authentication. According to OMB and DHS, “A single-factor authentication mechanism, such as a username and password, is insufficient to block even basic attackers.”⁵ Thus, strong information system authentication requires multiple factors to securely authenticate a user. Secure authentication requires something you have, something you are, and something you know. The President signed the implementation of Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, on August 27, 2004. This Presidential Directive requires all Federal agencies to use a standard badge for both physical and logical access. DHS indicated in its 2013 CIO and IG FISMA Reporting Metrics that the implementation of HSPD-12/PIV card is an “Administration Priority,” with two-factor authentication to be implemented Government-wide using PIV cards.

To manage the costs of implementing two-factor authentication for agency desktops and laptops, many Federal agencies are gradually implementing two-factor authentication as part of their desktop replacement cycle and migration from the Windows XP to Windows 7 operating system. Smaller Federal agencies are also leveraging Federal shared service providers and their technology infrastructure to significantly reduce the upfront costs of implementing two-factor authentication with PIV credentials. NIST states that small agencies may join with other agencies (and are encouraged to do so when cost-effective) to implement and use FIPS PUB 201 compliant⁶ components and systems.

Finding #6: Lack of Two-factor Authentication to the Corporation’s Desktops, Laptops, and Corporate Network

(See Appendix B, related DHS Question #3: Identity and Access Management)

Condition:

The Corporation’s laptops and desktops have not been configured to use PIV credentials for both physical and logical access control, as required by OMB Memoranda and NIST security guidance.

Cause:

OMB mandated the use of PIV cards for two-factor access without providing additional funding for its implementation. Moreover, IT budget decreases have left fewer resources available for implementing information security initiatives. Based on prior research, the Corporation determined that the cost of implementing two-factor authentication using a PIV card would be greater than the anticipated benefit.

⁵ *FY 2013 IG FISMA Reporting Metrics*, dated November 30, 2012, Question 3, “Identity and Access.”

⁶ FIPS PUB 201 is a Federal Government standard that specifies PIV requirements for Federal employees and contractors.

Criteria:

The President signed the implementation of HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, on August 27, 2004. This Presidential Directive requires all Federal agencies to use a standard badge for both physical and logical access. The purpose of a PIV badge is to "...support inter-agency interoperability" across the Federal Government.⁷ DHS indicated in its 2013 CIO and IG FISMA Reporting Metrics that the implementation of the HSPD-12/PIV card is an "Administration Priority" with two-factor authentication to be implemented Government-wide using PIV cards.

Further, NIST SP 800-53, Rev. 3 requires all Federal information systems to implement Security Control IA-2, "Identification and Authentication (Organization Users)," which states:

1. "The information system uses multifactor authentication for network access to privileged accounts.
2. The information system uses multifactor authentication for network access to non-privileged accounts.
3. The information system uses multifactor authentication for local access to privileged accounts."

Effect:

In addition to noncompliance with HSPD-12 requirements, the current single-factor authentication mechanisms (e.g., a user ID and password) are no longer sufficient to block even unsophisticated attacks, given the advances in computer power and password cracking techniques, thereby increasing the likelihood of penetration.

Recommendation:

Kearney recommends that the Corporation:

9. Research avenues to implement two-factor authentication, such as leveraging a Federal shared service provider to reduce upfront technology costs, lower per unit cost, and adopt a gradual, phased-deployment strategy to overcome current budget constraints.

⁷ FIPS PUB 201-1, *Personal Identity Verification of Federal Employees and Contractors*, dated March 2006.

APPENDIX A: MANAGEMENT'S RESPONSE

November 26, 2013

TO: Stuart Axenfeld
Assistant Inspector General Audit

FROM: Robert Velasco II /s/
Chief Operating Officer

SUBJECT: Request for Comments on the Office of the Inspector General's (OIG)
Draft Report: Federal Information Security Management Act (FISMA)
Independent Evaluation for FY 2013

This memorandum responds to your memo on this subject, dated November 15, 2013.

The Corporation for National and Community Service (CNCS) appreciates the opportunity to review the subject draft report and offers the following general comments. Comments regarding specific OIG findings and recommendations are attached. CNCS has also included a summary of its planned actions as a second attachment.

CNCS does not agree that its Information Assurance Program (IAP) is not in full compliance with FISMA legislation, applicable Office of Management and Budget (OMB) guidance, and NIST Special Publications (SPs). CNCS's method of compliance is based on the latitude that OMB provides to small agencies to adapt many of its regulations and guidelines developed for large agencies with multiple bureaus to the specific circumstances and resources of small agencies. Also, FISMA states that agencies are required to provide information security controls *proportionate with the risk and potential harm of not having those controls in place*. CNCS makes every effort to comply with the spirit of security guidance by careful tailoring its guidance to CNCS's risk assessments.

For example, OMB Memorandum M-05-24 (*Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*) specifically excludes government corporations, like CNCS, from the mandatory provisions of the memorandum. Instead, government corporations are encouraged, but not required, to implement the directive.

With respect to HSPD-12, CNCS has implemented PIV cards for physical access to the

Headquarters building and two-factor authentication for network access. As another example, CNCS has been at the vanguard of all Federal agencies in moving from NIST SP 800-53 (*Security and Privacy Controls for Federal Information Systems and Organizations*) revision 3 to revision 4.

The OIG has noted in several recent independent evaluations of the CNCS IAP, that CNCS has made great strides in improving its compliance with information security guidelines, with a view towards practical and effective controls over CNCS's systems and data. IAP policies, procedures and controls have all been developed and maintained within the context of the Program operations. CNCS has made the informed decision to selectively implement the full extent of documentation and management layers that are more appropriate to much larger organizations with semi-independent subordinate organizations.

CNCS has significantly improved its compliance with updated security guidelines. Now CNCS emphasis within the CNCS IAP is to turn to a broader, strategic view of information security, primarily to improve the support of cost-effective and risk-based resource decisions regarding future investment in information security.

The report notes in several places the 12 percent cut to CNCS's OIT budget for FY 2013 and implies that the CNCS information security program has been negatively affected as a result. On the contrary, the CNCS's resources (both staffing and funding) have been preserved. For example, a vacancy in the Chief Information Security Officer (CISO) position was immediately filled.

CNCS, through its IAP, has made information system and data security a high priority, and takes its responsibilities in this area seriously. Making good decisions about the effectiveness and risk/benefit assessments of security policy, processes, controls, investments, and oversights, is a continuing challenge as the IAP adapts to evolving CNCS missions and environmental threats. CNCS appreciates the OIG's perspective on its ability to meet those challenges and on its deliberate choices regarding the discretion CNCS has in implementing OMB and NIST guidelines.

If you have any questions or wish to discuss the comments on this draft report, please contact Lloyd Samples, CNCS CISO at 202-606-6662 or lsamples@cns.gov.

Attachments:

Agency Comments Regarding OIG Findings and Recommendations
Summary of Planned Agency Actions in Response to OIG Recommendations

cc: Philip Clark, Chief Information Officer
Guy Hadsall, OIG Chief Technology Officer

Agency Comments Regarding OIG Findings and Recommendations

Draft Report: OIG FISMA Independent Evaluation for FY 2013

Finding #1, Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy

The Cause section for Finding 1 misinterprets statements attributed to the Corporation for National and Community Service's (CNCS) Chief Information Officer (CIO). The relevant points the CIO was making are as follows:

- CNCS's continuous monitoring strategy is communicated through policy, procedure, guidance and oversight, much of which documented. CNCS does not rely on ad hoc daily practice to communicate and execute its continuous monitoring strategy.
- CNCS conducts continuous monitoring without the full-range of documentation contained in NIST guidance. The CIO did not intend to suggest that no documentation is needed.
- While OIT did absorb a 12 percent budget cut in FY 2013 due to sequestration, that budget cut in no way affected the staffing or funding of the Information Assurance Program.

The Criteria section for Finding 1 states that agencies are to implement continuous monitoring in lieu of the three-year security authorization and implies that CNCS's continued use of the three-year authorization is evidence of no continuous monitoring program. On the contrary, the Information Assurance Program continues to conduct three-year authorizations as an added layer of protection for CNCS on top of CNCS's continuous monitoring program. CNCS also improved on the three-year authorization cycle by conducting annual reviews of at least a third of a system's security controls each year, with 100% of them reviewed at least once within each three-year cycle.

CNCS interprets the intent of continuous monitoring guidance to shift agency reliance from a snapshot view of system security controls once every three years to a continuous or near-continuous monitoring stance to more quickly react to unusual activity or other security threats.

To that end, CNCS's enterprise-wide continuous monitoring process identifies and tracks the security state of its information technology assets. A few of the tools that CNCS uses to monitor network operations, client and server systems, and remote access in real time include:

1. CISCO MARS for Network Infrastructure
2. Good for Enterprise Security Mobility Solution
3. MaaS-360 Secure Mobile Device Management Suite for Android and IOS

4. Symantec Validation & ID Protection for two factor authentication of VPN
5. SolarWinds (seven different modules) for Network Operations

Ongoing security control assessments involve all appropriate stakeholders/officials in accordance with CNCS's continuous monitoring strategy. The continuous monitoring strategy also includes an effective configuration management process that assesses the security impact of any change to a system or its environment of operation.

CNCS has updated its organizationally-defined security requirements to reflect NIST SP 800-53, Revision 4. All systems are monitored for compliance with these requirements and IA policies, procedures, and Rules of Behavior.

Regarding Finding 1 recommendations, CNCS's information Assurance Program has begun to shift emphasis from security compliance to security strategy, primarily as a means to support effective security investments that will give CNCS maximum Agency-wide benefit. CNCS will ensure that documentation of strategy is improved in that process, will continue to document any corrective actions discovered in CNCS's POA&Ms, and will continue to ensure that the Information Assurance Program regularly reports on information security status to senior agency officials.

Finding #2, Lack of a Formally Documented and Fully Implemented Risk Management Framework (RMF)

Regarding the Condition section, CNCS has always approached information security management from a holistic perspective, including the CEO, COO, Program and Office Heads, and members of field offices in deliberations. Information security policies and practices resulting from those deliberations are briefed at all levels of CNCS.

Procedures are in place through CNCS's configuration control boards to ensure that the CISO reviews all proposed major business and technology changes to ensure that information security requirements are met, and to recommend alternative courses of action that will meet business needs while complying with information security requirements.

Risk assessment is never solely conducted at the information system level – all system security assessments and decisions are made in the context of the business use of data, higher level mitigating controls, etc.

As an example of adapting security requirements to business needs, CNCS deliberately provides devices on INCC campuses that do not link to the network and have minimal controls to provide business flexibility while meeting minimum security requirements.

Regarding the Cause section, the FY13 sequestration budget cuts for OIT have had no impact on base Information Security Program staffing or other resources.

Statements attributed to the agency CIO are also inaccurately presented. It is the CIO's position that adequate risk management strategies are in place and they are effectively documented through agency policy, procedures, etc. Also, rather than noting confusion, the CIO indicated disagreement with the auditors interpretation of narrower security controls as broader management internal controls that were beyond the scope of security controls. Specifically, that security controls at field locations should take into account perimeter physical security, but not direct physical security. Finally, contrary to report language, the CIO stated that, with regard to FISMA security controls, CNCS defines and manages risk at all levels within the agency.

Contrary to the report language, the CNCS CISO and eSPAN information system owner made a decision to delay the assessment due to the fact that the CNCS Network, from which eSPAN inherits a large percentage of its controls, was scheduled to undergo a complete authorization in calendar year 2013. Rather than conduct the annual eSPAN assessment as originally scheduled, a deliberate decision to provide an extension to the C&A was made to delay the partial security controls assessment that was scheduled within CY 2013 and pursue a more comprehensive eSPAN authorization shortly after completion of the Network authorization. Given that eSPAN and a number of eSPAN POA&M items from the previous year's security controls assessment had been addressed and that eSPAN was undergoing routine static code analysis scans (Fortify) as part of each software release, the eSPAN stakeholders determined that the risks of the delay were minimal. This postponement of 6 months avoided a major duplication of effort and was covered by an Interim Authority To Operate (IATO) that was based on an assessment of the risk associated with the delay and at no time has CNCS considered a multi-year postponement of authorization for any system for any reason.

Regarding the Effect section, CNCS's mission, technology adoption, and information security threat environment are all subject to constant change and constant security impact assessment. There is little risk that CNCS's risk management program will be "out of date". The Information Assurance Program will also coordinate closely with the CNCS Integrity Framework being developed by the Office of Accountability and Oversight (OAO) to enhance the agency's overall risk management process.

Barring evidence that CNCS's current multi-level, agency-wide risk management process is defective, adoption of a "formal" process for its own sake is not considered to be cost-justified.

CNCS will continue to obtain formal approval of waivers from policy and to establish, communicate, and execute appropriate disciplinary actions for violations of agency security policy.

Finding #3, Lack of a Fully Implemented Role-Based Information Security Training Program

The primary reason that draft role-based training modules have not been deployed is concern about their effectiveness, not the effects of budget cuts or competing priorities. Deployment has not been a high priority because CNCS already has a robust set of role-based security training activities:

- 1) Role based information sheets have been developed and are distributed at the same time as security appointments are made. These role sheets are also available on the CNCS intranet.
- 2) Individual meetings between Information Assurance staff and personnel with newly assigned information security roles are held at the time of designation to explain duties.
- 3) Privileged users and system administrators must read and agree to the CNCS regular and elevated Rules of Behavior (ROB). Information Assurance staff meet with all users given elevated privileges at the time of designation to explain duties.
- 4) The CNCS IA Policy includes a spreadsheet showing all the security controls and who is responsible for each control.
- 5) Enter on duty (EOD) and annual training is provided to all users including those with security responsibilities. The IA group participates at every EOD event and provides additional security guidance.

CNCS provides CNCS-specific security training to contractors with IS roles, but requires contractors to already have and maintain general qualifications and training for the roles they hold.

While it is always possible to provide more and better training, CNCS currently provides tailored, one-on-one training to users with information security roles. This actually meets a much higher standard than the generic role-based training modules that CNCS has not yet deployed.

CNCS agrees to provide better documentation of desk-side role-based training and may implement the draft generic role-based training modules if it can be determined to be an enhancement of the current training activities.

Finding # 4, Improvements Needed to Plan Of Actions & Milestones (POA&M) Reporting

The intent of OMB and NIST guidance regarding the POA&M process is to identify and track system vulnerabilities and other IS-related weaknesses and to ensure that adequate resources are allocated by the agency to address POA&M items. CNCS more than meets the intent of POA&M guidance.

Following the data breach in August 2010, the Corporation contracted with Booz Allen to conduct a static scan of agency code. That scan identified a number of potential vulnerabilities that included a large number of false positives. CNCS evaluated the scan results and identified a number of vulnerabilities ranging from low to critical. All vulnerabilities above moderate were mitigated with the highest priority. The remaining system vulnerabilities were captured on the eSPAN POA&M and the Corporation committed to allocating a significant portion of each quarterly software release to the resolution of open POA&M items. For each release, POA&M items are ranked for mitigation based on a number of factors, including the inherent risk level of the vulnerability, dependencies, and the economies of packaging certain "fixes" together, etc. All security-related changes are thoroughly tested by the OIT Quality Assurance Team to ensure that mitigations are successful. As a result of this

concerted effort, CNCS has, since March 2011, processed 57 security-related change requests that addressed more than 200 legacy application code vulnerabilities.

Just as important, CNCS invested in scanning software that is used for each release to ensure that new weaknesses are not introduced in new or modified code. No new weaknesses have been introduced since this process was implemented.

This ongoing success story leads CNCS to disagree with the OIG's assessment that there is significant risk that weaknesses will not be identified or resolved.

Additionally, the Corporation notes that OMB Memorandum M-02-01 (*Guidance for Preparing and Submitting Plans of Actions and Milestones (POA&Ms)*) does not specifically state that supporting evidence is required for closing open POA&Ms but, as often as possible, CNCS does try to include this information. Also, the same OMB Memorandum states that "... for each POA&M that relates to a project (including systems) for which a capital asset plan and justification (exhibit 300) was submitted or was a part of the exhibit 53, the unique project identifier must be reflected on the POA&M...". CNCS is not required to submit an exhibit 300, but it does submit an exhibit 53. However, the security section for exhibit 53 is no longer required per OMB Circular A-11. Even so, resources are tracked as part of CNCS's configuration management policy and procedures and labor hours are usually linked to eSPAN and Network POA&M entries even though it is not specially mandated.

The Corporation concurs with the recommendation to provide improved close-out documentation of POA&M items.

Finding #5, Improvements Needed to Ensure that Contractors Comply with the Corporation's Information Security Program Requirements

Neither the OIG or OIT staff could confirm the origin of Table 4 and it is not in current CNCS guidance. However, the content of the table is essentially accurate and is covered in various policies, procedures and training. The only exceptions are the April 15 report dates. To balance workload, those reports are now due annually on the anniversary date of the supporting contract's performance period.

CNCS typically does not identify specific tailoring of security controls in its acquisition documentation. Rather, CNCS requires contractors to submit a system security plan that recommends the tailoring of security controls appropriate to the system architecture, the contractor's environment, and the intended use cases. The proposed security plans that are tailored based on the complete set of security controls in NIST 800-53 rev 4 and the control recommendations are reviewed by the IA team, as well as by the CORs for appropriateness and completeness. Any concerns are resolved with contractors before accepting the deliverables as outlined in Section 6 of the IA clauses in the contract.

CNCS believes this process achieves acceptable levels of risk for CNCS and effectively identifies issues for resolution involving vendors.

CNCS agrees to review its IT acquisition policies, processes and training to ensure continued compliance with CNCS's security requirements.

Finding #6, Lack of Two-Factor Authentication to the Corporation's Desktops, Laptops, and Corporate Network

OMB Memorandum M-05-24 (*Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*) specifically excludes government corporations from the mandatory provisions of the memorandum. Government corporations are encouraged, but not required to implement the Directive.

In response to the intent of the directive, CNCS has implemented risk-adjusted 2-factor authentication solution:

- For physical access to the Headquarters building, CNCS has implemented a PIV badging system.
- For network access, all users must present a CNCS-approved device and provide correct user name and password to gain logical access.
- Remote users who are accessing the network from a non-CNCS device must present a secure and rotating system access code delivered via either software or hardware token, and provide a correct user name and password to gain logical access.

Providing 2-factor authentication using HSPD-12 cards for logical access to applications within the network has been considered. Providing that level access control has not been found to be cost-effective in the managed network environment or risk-justified compared to alternative monitoring and role-based access solutions that are currently in place.

CNCS will continue to research PIV for logical access, including possible shared service solutions.

Summary of Planned Corporation for National and Community Service (CNCS) Actions in Response to OIG Recommendations

Finding 1: Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy

No.	Recommendation	CNCS Comment	Planned CNCS Action
1	<p>Document and fully implement an ISCM strategy that incorporates the following:</p> <ul style="list-style-type: none"> a. Establishment of metrics to be monitored. b. Establishment of frequencies for monitoring/assessments. c. Ongoing security control assessments to determine the effectiveness of deployed security controls. d. Ongoing security status monitoring. e. Correlation and analysis of security-related information generated by assessments and monitoring. f. Response actions to address the results of the analysis. g. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137. 	<p>The recommendation implies implementation of the full range and depth of guidance contained in the NIST SP. CNCS has tailored guidance regarding ISCM based on its assessment of agency risks, mission, organization, size, etc.</p>	<p>CNCS will review its ISCM strategy in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.</p>

Finding 2: Lack of Formally Documented and Fully Implemented Risk Management Framework (RMF)

No.	Recommendation	CNCS Comment	Planned CNCS Action
2	Document and fully implement a process for addressing and capturing risk at the organization/mission, and business process levels throughout the organization.	CNCS incorporates a holistic approach to risk assessment to include all levels of the organization in making information assurance decisions, policies and investments, tailoring NIST guidance to agency needs.	CNCS will review its risk management framework in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.
3	Clearly assign ownership and responsibilities for executing risk management processes at the business/program level (Tier 2).	CNCS incorporates a holistic approach to risk assessment to include all levels of the organization in making information assurance decisions, policies and investments, tailoring NIST guidance to agency needs.	CNCS will review its risk management framework in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.
4	Ensure compliance with processes for monitoring security controls at the information system level (i.e., Tier 3), and obtain formal approval and necessary waivers for departures from Corporation policy. Further, establish and communicate potential disciplinary actions for noncompliance with the Corporation's security policies.	CNCS currently monitors security controls at the system level, prepares and approves waivers, and takes disciplinary action as appropriate.	CNCS will review its policy and processes in these areas in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.

Finding 3: Lack of a Fully Implemented of a Role-based Information Security Training Program

No.	Recommendation	CNCS Comment	Planned CNCS Action
5	Implement role-based security training for all users with significant information security responsibilities and maintain documentation for the completion of training.	CNCS provides written guidance and deskside training to all users with significant information security responsibilities.	CNCS will improve documentation of training given.

Finding 4: Improvements Needed to Plan Of Actions & Milestones (POA&M) Reporting

No.	Recommendation	CNCS Comment	Planned CNCS Action
6	Enhance the POA&M process to identify resources required for remediation either in the POA&M item or associated change request.	CNCS has a robust process and significant allocation of resources to aggressively mitigate POA&M items. Tracking of resource and implementation actions are shared between the POA&M and system change request processes.	CNCS will clarify the relationship between these two processes.
7	Strengthen the POA&M process to require individuals to reference evidence supporting the closure of a POA&M item.	CNCS has not been consistent in documenting evidence supporting closure of POA&M items.	CNCS will modify processes to ensure that evidence supporting closure of a POA&M item is consistently documented.

Finding 5: Improvements Needed to Ensure that Contractors Comply with the Corporation's Information Security Program Requirements

No.	Recommendation	CNCS Comment	Planned CNCS Action
8	Strengthen contractor oversight to ensure compliance with the Corporation's security requirements by clearly assigning oversight responsibility and required activities for Contracting Officers (CO), system owners, and supporting IT professionals.	CNCS provides adequate guidance to acquisition personnel and system owners regarding their responsibilities for requiring and overseeing information security requirements on IT contracts.	CNCS will review its IT acquisition policies, processes, and training regarding compliance with the CNCS's security requirements by IT contractors and make any appropriate adjustments to process or documentation as necessary.

Finding 6: Lack of Two-Factor Authentication to the Corporation's Desktops, Laptops and Corporate Network

No.	Recommendation	CNCS Comment	Planned CNCS Action
9	Research avenues to implement two-factor authentication, such as leveraging a Federal shared service provider to reduce upfront technology costs, lower per unit cost, and adopt a gradual, phased-deployment strategy to overcome current budget constraints.	CNCS has applied discretion granted by OMB and NIST guidance in its implementation of two-factor authentication. Two-factor authentication is already implemented for physical access to the HQ building and for logical access to the CNCS network (either on-site or remotely). CNCS does not consider it cost-effective to implement two-factor authentication for logical access to CNCS applications at this time.	CNCS will continue to evaluate options for two-factor authentication for logical access to Agency applications, taking into consideration potential shared services and phased implementation strategies.

APPENDIX B: KEARNEY’S AND OIG’S ANALYSIS OF PLANNED ACTIONS

On November 26, 2013, the Corporation for National and Community Service (Corporation) provided written responses (Appendix A) to the draft of this report. The Corporation agreed with the factual accuracy of all observations, but only partially agreed with recommended actions. The prevailing rationale for the partial agreement is that as a small Government corporation, the additional security controls required by the Office of Management and Budget (OMB) and National Institute of Standards and Technology (NIST) of larger, cabinet-level agencies were not appropriate or cost effective for the Corporation to implement. In this light, the Corporation agreed to consider the merits of our recommendations, but would generally not agree to implement them. In one instance, the Corporation cited an August 5, 2005 OMB Memorandum, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12*, as exempting Government corporations from implementing personal identity verification (PIV) cards for physical access and logical access to Government networks, desktops, and data. Subsequent memoranda from OMB⁸, NIST, and the Department of Homeland Security (DHS) do not provide an exemption for Government corporations to not implement the requirements of HSPD 12 and Federal Information Processing Standards (FIPS) Publication (PUB) 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, dated March 2006. For example, OMB Memorandum M-11-11, *Continued Implementation of HSPD-12-Policy for a Common Identification Standard for Federal Employees and Contractors*, dated February 3, 2011, mandates that all Federal agencies implement HSPD 12 and associated requirements for two-factor authentication using a PIV badge. The Corporation must determine if it is legally required to implement PIV cards for both physical and logical access to the network. Regardless, it is widely recognized by information security professionals that two-factor authentication is an industry best practice, provides superior identification and authentication of users, and can thwart attacks to capture a user’s ID and password.

In the following tables, Kearney and the OIG evaluated the Corporation’s response for each of the six findings and determined if the Corporation’s planned actions were responsive to the recommendation. Kearney defined responsive as follows:

- **Yes** indicates that planned actions fully address the noted weakness and root cause.
- **No** indicates that planned actions do not address the noted weakness and root cause.
- **Partial** indicates that planned actions do not fully address the noted weakness and additional actions are necessary.

⁸ Since 2002, OMB issues annual Federal Information Security Management Act (FISMA) reporting instructions for agencies’ Chief Information Officers (CIO), Senior Agency Official for Privacy, and Inspector Generals. The annual FISMA reporting instructions clarify OMB’s interpretation of the FISMA legislation and include a Frequently Asked Questions (FAQ) section to explain OMB policy. The most recent OMB FISMA reporting instructions were issued on November 18, 2013 (OMB Memorandum M-14-04). OMB clearly states that the Federal Information Processing Standards (FIPS) may not be waived by Federal agencies (Question 11, page 5). The FAQs section does not provide any exemption for Government corporations to not implement PIV badges for both physical and logical access.

The following items will remain open until follow-up is conducted in the fiscal year (FY) 2014 FISMA evaluation and the Office of Inspector General (OIG) determines that agreed-upon corrective actions are complete and responsive.

Finding 1: Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
1	<p>Document and fully implement an ISCM strategy that incorporates the following:</p> <ul style="list-style-type: none"> a. Establishment of metrics to be monitored b. Establishment of frequencies for monitoring/assessments c. Ongoing security control assessments to determine the effectiveness of deployed security controls d. Ongoing security status monitoring e. Correlation and analysis of security-related information generated by assessments and monitoring f. Response actions to address the results of the analysis g. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST Special Publication (SP) 800-137. 	<p>The recommendation implies implementation of the full range and depth of guidance contained in the NIST SP. CNCS has tailored guidance regarding ISCM based on its assessment of agency risks, mission, organization, size, etc.</p>	<p>CNCS will review its ISCM strategy in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.</p>	<p>Responsive: Partial</p> <p>Kearney agrees that the Corporation’s planned action is an appropriate first step; however, the Corporation does not agree to document its ISCM strategy and identify key security metrics. Kearney continues to make the recommendation as stated.</p>

Finding 2: Lack of Formally Documented and Fully Implemented Risk Management Framework (RMF)

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
2	<p>Document and fully implement a process for addressing and capturing risk at the organization, mission, and business</p>	<p>CNCS incorporates a holistic approach to risk assessment to include all</p>	<p>CNCS will review its risk management framework in light of OIG recommendations and</p>	<p>Responsive: Partial</p> <p>Kearney agrees that the Corporation’s planned action is an appropriate first</p>

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
	process levels throughout the organization.	levels of the organization in making information assurance decisions, policies, and investments, and tailors NIST guidance to agency needs.	make any appropriate adjustments to processes or documentation as necessary.	step; however, the Corporation does not agree to document its risk management approach and consider Levels I and II in its methodology, consistent with NIST SP 800-37, Revision (Rev.) 1, <i>Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach</i> . Kearney continues to make the recommendation as stated.
3	Clearly assign ownership and responsibilities for executing risk management processes at the business/program level (Tier 2).	CNCS incorporates a holistic approach to risk assessment to include all levels of the organization in making information assurance decisions, policies and investments, tailoring NIST guidance to agency needs.	CNCS will review its risk management framework in light of OIG recommendations and make any appropriate adjustments to process or documentation as necessary.	Responsive: Partial Kearney agrees that the Corporation's planned action is an appropriate first step; however, the Corporation does not agree to document and clearly assign roles and responsibilities for risk management functions at the business level. Kearney continues to make the recommendation as stated.
4	Ensure compliance with processes for monitoring security controls at the information system level (i.e., Tier 3), and obtain formal approval and necessary waivers for departures from Corporation policy. Further, establish and communicate potential disciplinary actions for noncompliance with the Corporation's security policies.	CNCS currently monitors security controls at the system level, prepares and approves waivers, and takes disciplinary action as appropriate.	CNCS will review its policies and processes in these areas in light of OIG recommendations and make any appropriate adjustments to processes or documentation as necessary.	Responsive: Partial Kearney acknowledges the cost justification in delaying the application risk assessment and encourages the Corporation to document its risk acceptance and departure from Corporate policy when such events occur. In the case of eSPAN, the Corporation should complete the risk assessment. Kearney continues to make the recommendation as stated.

Finding 3: Lack of a Fully Implemented Role-Based Information Security Training Program

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
5	Implement role-based security training for all users with significant information security responsibilities and maintain documentation for the completion of training.	CNCS provides written guidance and desk side training to all users with significant information security responsibilities.	CNCS will improve documentation of training given.	Responsive: Partial Kearney agrees that documenting role-based training provided to individuals with significant information security responsibility is one action of several needed. Other key actions include delivering role-based security training to the Corporation's IT professionals, Contracting Officers, System Owners, and other employees involved in the oversight of the Corporation's IT vendors to ensure that all parties understand and follow the Corporation's security policies. Kearney continues to make the recommendation as stated.

Finding 4: Improvements Needed to Plans of Actions and Milestones (POA&M) Reporting

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
6	Enhance the POA&M process to identify resources required for remediation either in the POA&M item or the associated change request ticket.	CNCS has a robust process and significant allocation of resources to aggressively mitigate POA&M items. Tracking of resource and implementation actions are shared between the POA&M and system change request processes.	CNCS will clarify the relationship between these two processes.	Responsive: Partial Kearney agrees that the Corporation's planned action is an appropriate first step; however, the Corporation did not agree to estimate resources required to resolve noted security weaknesses captured on either a POA&M or a change request. Kearney believes this is essential information for tracking and communicating resource needs to Corporation Executives when establishing the annual budget for the Corporation's information

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
				security program. Kearney continues to make the recommendation as stated.
7	Strengthen the POA&M process to require individuals to reference evidence supporting the closure of a POA&M item.	CNCS has not been consistent in documenting evidence supporting closure of POA&M items.	CNCS will modify processes to ensure that evidence supporting closure of a POA&M item is consistently documented.	Responsive: Yes The Corporation concurred with the recommendation to provide improved close-out documentation of POA&M items.

Finding 5: Improvements Needed to Ensure that Contractors Comply with the Corporation's Information Security Program Requirements

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
8	Strengthen contractor oversight to ensure compliance with the Corporation's security requirements by clearly assigning oversight responsibility and required activities for Contracting Officers (CO), system owners, and supporting information technology (IT) professionals.	CNCS provides adequate guidance to acquisition personnel and system owners regarding their responsibilities for requiring and overseeing information security requirements on IT contracts.	CNCS will review its IT acquisition policies, processes, and training regarding compliance with the CNCS's security requirements by IT contractors and make any appropriate adjustments to processes or documentation, as necessary	Responsive: Partial Kearney agrees that the Corporation's planned action is an appropriate first step; however, the Corporation did not agree to take any specific action or clarify responsibilities of CO and system owners with regard to external IT providers. Kearney continues to make the recommendation as stated.

Finding 6: Lack of Two-Factor Authentication to the Corporation's Desktops, Laptops, and Corporate Network

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
9	Research avenues to implement two-factor authentication, such as leveraging a Federal shared service provider to reduce upfront technology costs, lower per unit cost, and adopt a gradual, phased-deployment strategy to overcome current budget constraints.	CNCS has applied discretion granted by OMB and NIST guidance in its implementation of two-factor authentication. Two-factor authentication is already implemented for	CNCS will continue to evaluate options for two-factor authentication for logical access to Agency applications, taking into consideration potential shared services and phased implementation	Responsive: Partial Kearney recommends that the Corporation incorporate the plan of action as defined in OMB Memorandum M-11-11, <i>Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a</i>

No.	Recommendation	Corporation Comment	Planned Corporation Action	Evaluator Analysis
		<p>physical access to the HQ building and for logical access to the CNCS network (either on-site or remotely).CNCS does not consider it cost-effective to implement two-factor authentication for logical access to CNCS applications at this time.</p>	<p>strategies.</p>	<p><i>Common Identification Standard for Federal Employees and Contractors.</i> Kearney continues to make the recommendation as stated.</p>

APPENDIX C: RESPONSES TO DHS’S FY 2013 IG FISMA REPORTING METRICS

FY 2013 IG FISMA Metrics

1: CONTINUOUS MONITORING MANAGEMENT		Answer
<i>Please select Yes or No from the pull down menu.</i>		
1.1.	Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?	No
1.1.1.	Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). (AP)	No
1.1.2.	Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev. 1, Appendix G). (AP)	No
1.1.3.	Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST SP 800-53A). (AP)	Yes
1.1.4.	Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, NIST SP 800-53A). (AP)	Yes
1.2 Please provide any additional information on the effectiveness of the organization’s Continuous Monitoring Management Program that was <u>not noted</u> in the questions above.		
1.2 Response: Current policies and procedures for continuous monitoring can be improved through the implementation of an Information Security Continuous Monitoring Strategy that considers all activities at the organization, mission/business process, and information systems tiers. The Corporation for National and Community Service (Corporation) identified the need for the development of an Information Security Continuous Monitoring Strategy for each system in its Information Assurance Strategic Plan, dated October 2012.		
2: CONFIGURATION MANAGEMENT		Answer
<i>Please select Yes or No from the pull down menu.</i>		
2.1	Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?	Yes
2.1.1.	Documented policies and procedures for configuration management. (Base)	Yes
2.1.2.	Defined standard baseline configurations. (Base)	Yes

2: CONFIGURATION MANAGEMENT		Answer
<u>Please select Yes or No from the pull down menu.</u>		
2.1.3.	Assessments of compliance with baseline configurations. (Base)	Yes
2.1.4.	Process for timely (as specified in organization policy or standards) remediation of scan result deviations. (Base)	Yes
2.1.5.	For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. (Base)	Yes
2.1.6.	Documented proposed or actual changes to hardware and software configurations. (Base)	Yes
2.1.7.	Process for timely and secure installation of software patches. (Base)	Yes
2.1.8.	Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). (Base)	Yes
2.1.9.	Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). (Base)	Yes
2.1.10.	Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53: CM-3, SI-2). (Base)	Yes
2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was <u>not noted</u> in the questions above.		
2.2 Response: No additional information.		

3: IDENTITY AND ACCESS MANAGEMENT		Answer
<u>Please select Yes or No from the pull down menu.</u>		
3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?		Yes
3.1.1.	Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). (Base)	Yes
3.1.2.	Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). (Base)	Yes

3: IDENTITY AND ACCESS MANAGEMENT		Answer
<i>Please select Yes or No from the pull down menu.</i>		
3.1.3.	Identifies when special access requirements (e.g., multi-factor authentication) are necessary. (Base)	Yes
3.1.4.	If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). (KFM)	Yes
3.1.5.	Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)	Yes
3.1.6.	Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).	Yes
3.1.7.	Ensures that the users are granted access based on needs and separation-of-duties principles. (Base)	Yes
3.1.8.	Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) (Base)	Yes
3.1.9.	Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) (Base)	Yes
3.1.10.	Ensures that accounts are terminated or deactivated once access is no longer required. (Base)	No
3.1.11.	Identifies and controls use of shared accounts. (Base)	No
3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was <u>not noted</u> in the questions above.		
3.2 Response: Due to budget cuts, the Corporation has elected not to implement two-factor authentication for access to the Corporation's desktops, servers, and network devices. The Corporation has begun deployment of Homeland Security Presidential Directive (HSPD)-12 badges to Federal employees; however, the implementation is limited to physical access to the Corporation's Headquarters building. Additionally, Kearney & Company, P.C. (Kearney) noted that there is a prior year (PY) Notification of Finding and Recommendation (NFR) for inactive accounts that have not been disabled and/or removed. Kearney noted that this has been identified and tracked on the system Plan of Actions and Milestones (POA&M). The status of this action item is "ongoing."		

4: INCIDENT RESPONSE AND REPORTING		Answer
<u>Please select Yes or No from the pull down menu.</u>		
4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
4.1.1.	Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1). (Base)	Yes
4.1.2.	Comprehensive analysis, validation, and documentation of incidents. (KFM)	Yes
4.1.3.	When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (KFM)	Yes
4.1.4.	When applicable, reports to law enforcement within established timeframes (SP 800-61). (KFM)	Yes
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, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (KFM)	Yes
4.1.6.	Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. (Base)	No
4.1.7.	Is capable of correlating incidents. (Base)	Yes
4.1.8.	Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (Base)	Yes
4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was <u>not noted</u> in the questions above.		
4.2 Response: The Corporation does not currently utilize any Cloud Service Providers. As such, Question 4.1.6 is not applicable to the Corporation.		

5: RISK MANAGEMENT		Answer
<u>Please select Yes or No from the pull down menu.</u>		
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?		No
5.1.1.	Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)	Yes
5.1.2.	Addresses risk from an <u>organization perspective</u> with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (Base)	No

5: RISK MANAGEMENT		Answer
<i>Please select Yes or No from the pull down menu.</i>		
5.1.3.	Addresses risk from a <u>mission and business process perspective</u> and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1. (Base)	No
5.1.4.	Addresses risk from an <u>information system perspective</u> 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)	Yes
5.1.5.	Has an up-to-date system inventory. (Base)	Yes
5.1.6.	Categorizes information systems in accordance with government policies. (Base)	Yes
5.1.7.	Selects an appropriately tailored set of baseline security controls. (Base)	Yes
5.1.8.	Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)	No
5.1.9.	Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)	No
5.1.10.	Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)	No
5.1.11.	Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)	No
5.1.12.	Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. (Base)	No
5.1.13.	Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). (Base)	Yes
5.1.14.	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. (Base)	No
5.1.15.	Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18, NIST SP 800-37). (Base)	Yes
5.1.16.	Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. (Base)	Yes

5: RISK MANAGEMENT		Answer
<u>Please select Yes or No from the pull down menu.</u>		
5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was <u>not noted</u> in the questions above.		
5.2 Response: The Corporation has not developed a Risk Management Program consistent with Federal Information Security Management Act of 2002 (FISMA) requirements, Office of Management and Budget (OMB) policy, and applicable National Institute of Standards and Technology (NIST) guidelines. Specifically, the Corporation has not implemented the NIST Risk Management Framework (RMF), as described in NIST Special Publication (SP) 800-37, Revision (Rev.) 1; and NIST SP 800-39 at the Tier 1: Organizational and Tier 2: Mission/Business levels.		

6: SECURITY TRAINING		Answer
<u>Please select Yes or No from the pull down menu.</u>		
6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
6.1.1.	Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). (Base)	Yes
6.1.2.	Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)	Yes
6.1.3.	Security training content based on the organization and roles, as specified in organization policy or standards. (Base)	No
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)	Yes
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)	No
6.1.6.	Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, NIST SP 800-53). (Base)	Yes
6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was <u>not noted</u> in the questions above.		
6.2 Response: The Corporation identified the need for the development of a role-based training program in its Information Assurance Strategic Plan, dated October 2012. The Corporation has documented information technology (IT) security training policies and procedures; however, it has not implemented these training procedures and practices for individuals with significant information security responsibilities. The retirement of the Chief Information Security Officer (CISO) and a 12% reduction in the IT budget has limited the Corporation's ability to implement new IT initiatives with existing resources.		

7: PLAN OF ACTIONS AND MILESTONES (POA&M)		Answer
<i>Please select Yes or No from the pull down menu.</i>		
7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
7.1.1.	Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. (Base)	Yes
7.1.2.	Tracks, prioritizes, and remediates weaknesses. (Base)	Yes
7.1.3.	Ensures remediation plans are effective for correcting weaknesses. (Base)	Yes
7.1.4.	Establishes and adheres to milestone remediation dates. (Base)	No
7.1.5.	Ensures resources and ownership are provided for correcting weaknesses. (Base)	No
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)	Yes
7.1.7.	Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3; OMB M-04-25). (Base)	No
7.1.8.	Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25). (Base)	Yes
7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was <u>not noted</u> in the questions above.		
7.2 Response: The Corporation has policies and procedures for managing its POA&Ms; however, it has not consistently implemented these policies and procedures. Kearney noted that resources and costs were not consistently estimated and reported in POA&Ms. Additionally, the existence of overdue milestones suggests that corrective actions were not consistently implemented as scheduled, and periodic updates to the POA&Ms were not performed to reflect new operational challenges and milestone delays.		

8: REMOTE ACCESS MANAGEMENT		Answer
<i>Please select Yes or No from the pull down menu.</i>		
8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
8.1.1.	Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17). (Base)	Yes
8.1.2.	Protects against unauthorized connections or subversion of authorized connections. (Base)	Yes

8: REMOTE ACCESS MANAGEMENT		Answer
<u>Please select Yes or No from the pull down menu.</u>		
8.1.3.	Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). (Base)	Yes
8.1.4.	Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)	Yes
8.1.5.	If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3). (KFM)	Yes
8.1.6.	Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)	Yes
8.1.7.	Defines and implements encryption requirements for information transmitted across public networks. (KFM)	Yes
8.1.8.	Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. (Base)	No
8.1.9.	Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). (Base)	Yes
8.1.10.	Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). (Base)	No
8.1.11.	Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6). (Base)	No
8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was <u>not noted</u> in the questions above.		
8.2 Response: The Corporation does not have a Rules of Behavior Form specific to remote access management. The general Rules of Behavior Form does include guidelines for remote access. Additionally, the Corporation is in process of revising security requirements for session time-outs to 15 minutes of inactivity.		
8.3	Does the organization have a policy to detect and remove unauthorized (rogue) connections?	Yes

9: CONTINGENCY PLANNING		Answer
<u>Please select Yes or No from the pull down menu.</u>		
9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
9.1.1.	Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1). (Base)	Yes
9.1.2.	The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). (Base)	Yes

9: CONTINGENCY PLANNING		Answer
<i>Please select Yes or No from the pull down menu.</i>		
9.1.3.	Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). (Base)	No
9.1.4.	Testing of system-specific contingency plans. (Base)	No
9.1.5.	The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)	Yes
9.1.6.	Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	No
9.1.7.	Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. (Base)	No
9.1.8.	After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)	No
9.1.9.	Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.10.	Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).	Yes
9.1.11.	Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.12.	Contingency planning that considers supply chain threats. (Base)	No
9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was <u>not noted</u> in the questions above.		
9.2 Response: Detailed testing of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) was conducted during the current year. The Corporation and SRA International, Inc. (SRA) have DRPs for the SRA Managed Data Center Services (MDCS) and at Savvis; however, testing of controls for the Electronic System for Programs, Agreements, and National Service (eSPAN) is currently in process and has not been performed for this current year because the application security assessment is currently in process. This application is operating under an extended authority to operate. Further, documentation evidencing a simulated disaster scenario or a "table top" exercise was not provided.		

10: CONTRACTOR SYSTEMS		Answer
<i>Please select Yes or No from the pull down menu.</i>		
10.1.	Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?	Yes
10.1.1.	Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud. (Base)	Yes
10.1.2.	The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2). (Base)	No

10: CONTRACTOR SYSTEMS		Answer
<i>Please select Yes or No from the pull down menu.</i>		
10.1.3.	A complete inventory of systems operated on the organization’s behalf by contractors or other entities, including organization systems and services residing in a public cloud. (Base)	Yes
10.1.4.	The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). (Base)	Yes
10.1.5.	The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. (Base)	Yes
10.1.6.	The inventory of contractor systems is updated at least annually. (Base)	Yes
10.1.7.	Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)	Yes
10.2 Please provide any additional information on the effectiveness of the organization’s Contractor Systems Program that was <u>not noted</u> in the questions above.		
10.2 Response: The Corporation has developed security policies requiring Contracting Officers (CO) and their technical representatives to conduct oversight and monitoring of their contractors’ adherence to Corporation security policies. However, the Corporation could not provide evidence of this monitoring and adherence to agency policy.		

11: SECURITY CAPITAL PLANNING		Answer
<i>Please select Yes or No from the pull down menu.</i>		
11.1. Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
11.1.1.	Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. (Base)	Yes
11.1.2.	Includes information security requirements as part of the capital planning and investment process. (Base)	Yes
11.1.3.	Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). (Base)	Yes
11.1.4.	Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). (Base)	Yes
11.1.5.	Ensures that information security resources are available for expenditure as planned. (Base)	Yes
11.2 Please provide any additional information on the effectiveness of the organization’s Security Capital Planning Program that was <u>not noted</u> in the questions above.		
11.2 Response: According to the Corporation’s management, the Corporation is not required to prepare Exhibit 300, as the Corporation is considered a small agency for the purposes of FISMA.		

APPENDIX D: RESULTS FROM NCCC AND STATE FIELD OFFICE ASSESSMENTS

Field office assessments were conducted at the Jackson State Office and National Civilian Community Corps (NCCC)-Vicksburg and NCCC-Perry Point. As part of Kearney & Company, P.C.'s (Kearney) assessment strategy, workspace and office suite areas were inspected for personally identifiable information (PII) exposures. Kearney's visits to these locations also included an evaluation of workstation configuration and encryption, evaluation of controls to ensure acceptable usage of Corporation for National and Community Service (Corporation) network resources, physical security, rogue connections, PII management, and a search for inappropriate material on Corporation workstations.

At the Jackson State Office, Kearney toured the State Office and noted that PII (paper and portable electronic) was adequately stored and protected. Physical access controls to the facility and State Office work area appeared to be sufficient, considering the State Office's mission and known threats. Kearney did not detect any wireless access points within proximity of the State Office. Kearney noted that SRA International, Inc. (SRA) deployed technology to manage the configuration of the Corporation's laptops and deploy security patches. Based on an un-credentialed vulnerability scan with the vulnerability tool, Nessus, these laptops appeared to be sufficiently protected with an active personal firewall.

Kearney noted opportunities to improve site controls by formally evaluating risks at field locations, establishing baseline controls, defining selected controls in a site-specific Security Program Plan, and establishing an oversight program for field locations.

Field Office Scans

The Kearney Federal Information Security Management Act of 2002 (FISMA) Evaluation Team conducted scans to assess site compliance with the Federal Desktop Core Configuration (FDCC) and United States Government Compliance Baseline (USGCB) requirements. In order to perform this task, Kearney employed the Nessus scanning tool with FDCC USGCB plug-ins to scan laptop and desktop computer configurations for all devices at each location.

Scope Limitation

During the site visits, Kearney determined that the Corporation's network security configuration would not permit on-site compliance scanning for the SRA-managed desktops and network devices using authenticated credentials (i.e., user ID and password). With the Office of Inspector General's (OIG) concurrence, Kearney and SRA agreed that subsequent scans would occur at the end of the FISMA evaluation and be conducted remotely from the Corporation's Headquarters in Washington, D.C. The test results of these scans and associated findings are not included within the scope of this report.

The OIG has determined that a separate Management Letter will be issued to bring to management's attention Kearney's concerns over the Corporation's oversight processes for field offices.

APPENDIX D: ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Plan
CEO	Chief Executive Officer
CIO	Chief Information Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CISO	Chief Information Security Officer
CO	Contracting Officer
Corporation	Corporation for National and Community Service
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
E-Gov	E-Government Act of 2002
eSPAN	Electronic System for Programs, Agreements, and National Service
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IAP	Information Assurance Program
ID	Identification
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
Kearney	Kearney & Company, P.C.
MDCS	Managed Data Center Services
NCCC	National Civilian Community Corps
NFR	Notification of Finding and Recommendation
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
POA&M	Plan of Actions and Milestones
PUB	Publication
PY	Prior Year
Rev.	Revision
RMF	Risk Management Framework
SP	Special Publication
SRA	SRA International, Inc.
USGCB	United States Government Compliance Baseline

APPENDIX E: REFERENCED DOCUMENTS

Federal Information Security Management Act of 2002 (FISMA) (Title III, Public Law [P.L.] No. 107-347)

Office of Management and Budget (OMB):

- Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- Memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- Memorandum M-06-15, *Safeguarding Personally Identifiable Information*
- Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.*

Federal Information Processing Standards (FIPS):

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

National Institute of Standards and Technology (NIST) Special Publications (SP):

- 800-18, Revision (Rev.) 1, *Guide for Developing Security Plans for Federal Information Systems*
- 800-30, *Risk Management Guide for Information Technology Systems*
- 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
- 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
- 800-60, Rev. 1, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*
- 800-83, *Guide to Malware Incident Prevention and Handling*
- 800-100, *Information Security Handbook: A Guide for Managers.*

If you want to report or discuss confidentially any instance of misconduct, fraud, waste, abuse, or mismanagement, please contact the Office of Inspector General.

Telephone:
The Inspector General's HOTLINE
(800) 452-8210

The deaf or hard of hearing, dial FRS (800) 877-8339 and give the Hotline number to the relay operator.

Web:
<http://www.cncsoig.gov/hotline>

Or Write:
Corporation for National and Community Service
Office of Inspector General
1201 New York Ave, NW
Suite 830
Washington, DC 20525
(202) 606-9390