Office of Inspector General
Corporation for National and Community Service

FISCAL YEAR 2015
FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT 16-03

Prepared by:

Kearney & Company, P.C.
1701 Duke Street, Suite 500
Alexandria, Virginia 22314

This report was issued to Corporation management on November 13, 2015. 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 May 13, 2016, and complete its corrective actions by November 14, 2016. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Office of Inspector General
Corporation for NATIONAL & COMMUNITY SERVICE

November 13, 2015

TO: Wendy Spencer
Chief Executive Officer

FROM: Stuart Axenfeld */s/*
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2015 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service (OIG Report 16-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 16-03, *Fiscal Year 2015 Federal Information Security Modernization Act Evaluation of 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 concluded that the Corporation's Information Security and Privacy Program was not compliant in a number of respects with FISMA legislation, Office of Management and Budget guidance, and applicable National Institute of Standards and Technology security publications as of September 30, 2015. Their testing found the controls were ineffective in eight of the 11 areas. In two of the eight areas, the deficiencies were severe enough to constitute a significant deficiency; these areas were Continuous Monitoring Management and Risk Management.

Should you have any questions about this report, please contact Guy Hadsall, Chief Technology Officer, at 202-606-9375; Thomas Chin, Audit Manager, at 202-606-9362; or me at 202-606-9360.

Attachment

cc: Asim Mishra, Chief of Staff
Jeremy Joseph, General Counsel
Jeffrey Page, Chief Operating Officer and Acting Chief Financial Officer
Tom Hanley, Chief Information Officer
Kathryn Gillis, Director, Office of Accountability and Oversight
Tyler Harding, Engagement Principal, Kearney & Company, P.C.

Fiscal Year 2015 Federal Information Security Modernization Act Evaluation for the

Corporation for National and Community Service

November 13, 2015

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

OIG Highlights

Objective

FISMA requires each Federal agency to undergo an annual independent evaluation of its information security program and practices. The OIG contracted with Kearney to conduct the FY 2015 FISMA evaluation of the Corporation. The objectives were to evaluate a representative subset of the Corporation's information systems for compliance with FISMA, Office of Management and Budget (OMB), and National Institute of Standards and technology (NIST) guidance, and to evaluate the operating effectiveness of the information security and privacy controls over those systems.

Recommendations

Resolving serious security and privacy weaknesses throughout the Corporation's information security and privacy program will require a disciplined and sustained effort, as well as a commitment of substantial resources.

The Corporation has begun, but not yet implemented, the four key prior year recommendations. The OIG recommends that the Corporation take four key steps:

(1) Establish an IT project to prioritize and remedy the weaknesses, led by the CISO
(2) Develop a Project Plan with specific milestones and assignments of responsibility
(3) Identify and marshal the resources, skills, and expertise necessary to implement the Project Plan
(4) Establish performance metrics for information security oversight and obtain support from agency leadership.

November 2015

Weaknesses Identified in the Corporation's Information Security and Privacy Program

Office of Inspector General
Corporation for NATIONAL & COMMUNITY SERVICE

What the OIG Found

The Corporation for National and Community Service (the Corporation) has taken a number of meaningful steps to address information security and privacy weaknesses from the fiscal year (FY) 2014 Federal Information Security Management Act of 2002 (FISMA) evaluation: resolving three out of sixteen findings from the FY 2014 evaluation and hiring a Chief Information Security Officer (CISO) and Security Analyst in June 2015 to support the development of the Corporation's Information Security Program. Additionally, the Corporation established a Memorandum of Agreement (MOA) in November 2014 with the Department of Homeland Security (DHS) to participate in DHS's Continuous Diagnostics and Mitigation (CDM) Program.

Despite these preliminary steps, progress towards resolving fundamental weaknesses within the Corporation's Information Security Program has been limited, and serious vulnerabilities remain. Kearney & Company, P.C. (Kearney), under the Office of Inspector General's (OIG) supervision, identified new or continuing weaknesses in all 11 areas tested. The controls were found to be ineffective in eight of these areas, and, in two of them (i.e., Continuous Monitoring Management and Risk Management), the defects were severe enough to constitute a significant deficiency, warranting immediate corrective action and attention by agency leadership. Eight of these findings were reoccurring from the FY 2014 evaluation. Kearney also uncovered four new weaknesses: (1) information technology (IT) procurement; (2) access controls; (3) strategic planning, and (4) inventory management. Responses to DHS's 100 security metric questions identified 54 instances of noncompliance with applicable laws, regulations, and authoritative guidance governing information security. Kearney also found significant weaknesses in the Corporation's privacy controls for protection of Personally Identifiable Information (PII).

FY 2015 FISMA Evaluation Results

2015 DHS IG FISMA Reporting Area and Privacy	# of DHS Exceptions / Total DHS IG Questions	Severity of Noted Exceptions
1. Continuous Monitoring Management	8 of 8[1]	Significant Deficiency
2. Configuration Management	9 of 12	Control Deficiency
3. Identity and Access Management	1 of 9	Control Deficiency
4. Incident Response and Reporting	2 of 8	Control Deficiency
5. Risk Management	9 of 16	Significant Deficiency
6. Security Training	3 of 7	Control Deficiency
7. POA&Ms	6 of 9	Control Deficiency
8. Remote Access Management	3 of 12	Control Deficiency
9. Contingency Planning	10 of 12	Control Deficiency
10. Contractor Systems	3 of 7	Control Deficiency
†Privacy	N/A	Control Deficiency

† – Consistent with the addition of privacy controls to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, the OIG contracted with Kearney to evaluate the Corporation's implementation of specific privacy controls as part of the FY 2015 FISMA evaluation.
[1] – To enable comparison of this year's results with those of FY 2014, Kearney analyzed this year's Continuous Monitoring Management using the same eight Continuous Monitoring Management questions applicable in FY 2014. However, a new standard for assessing Continuous Monitoring Management, using a maturity model, went into effect on June 19, 2015, and Kearney assessed the Corporation's Continuous Monitoring Management under that standard. The maturity model yields the Corporation a score of "1 – Ad Hoc" in each of the three areas (People, Process, and Technology) evaluated.

In response to the OIG's FISMA report, the Corporation agreed to devote the resources and management attention to resolve the noted weakness and strengthen its Information Security Program. OIG looks forward to working with management to address these weaknesses.

TABLE OF CONTENTS

KEARNEY& COMPANY

1701 Duke Street, Suite 500, Alexandria, VA 22314
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

1. COVER LETTER

November 13, 2015

Wendy Spencer
Chief Executive Officer
Corporation for National and Community Service 1201
New York Avenue, NW, Washington, D.C. 20525

Dear Ms. Spencer:

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 (defined as "the Corporation") Information Security Program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires Federal agencies 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 other source. Additionally, FISMA mandates that the Corporation undergo an annual independent evaluation of its Information Security Program and practices, as well as an assessment of its compliance with the requirements of FISMA. The Corporation's Office of Inspector General (OIG) contracted with Kearney to perform an independent fiscal year (FY) 2015 FISMA evaluation of the Corporation's information technology (IT) policies, procedures, and practices. We are pleased to provide this FY 2015 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
- Assess the Corporation's compliance with FISMA and related information security policies, procedures, standards, and guidelines
- Evaluate protection over personally identifiable information (PII) and IT assets at the Corporation, including its field offices
- Prepare the Corporation's responses to the *Department of Homeland Security's (DHS) FY 2015 Inspector General (IG) Federal Information Security Modernization Act Reporting Metrics v1.2*, dated June 19, 2015 (referred to as the *DHS FY 2015 IG FISMA Reporting Metrics* in this report)
- Follow up on findings reported in previous FISMA evaluations to determine whether risks have been properly mitigated.

KEARNEY& COMPANY

Kearney's methodology for the FY 2015 FISMA evaluation included testing a sample of security controls over the Corporation's General Support System (GSS), local area network (LAN) and wide area network (WAN), and major applications (i.e., Electronic-System for Programs, Agreements, and National Service Participants [eSPAN] and Momentum Financial Management System [Momentum]) for compliance with the National Institute of Standards and Technology's (NIST) Special Publications (SP) and Office of Management and Budget (OMB) guidance. We placed particular emphasis on NIST SP 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Our evaluation was performed in accordance with the *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency (CIGIE),[1] and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

Since the FY 2014 FISMA evaluation, the Corporation has taken steps to improve its overall Information Security Program and its compliance with the FISMA legislation, OMB guidance, and applicable NIST SPs. The Corporation closed three out of 16 findings from the FY 2014 FISMA evaluation (i.e., "Lack of Controls to Prevent Use of Unauthorized Devices," "Lack of Segregation of Duties," and "Inadequate Incident Response Reporting"). Further, the Corporation hired a new Chief Information Security Officer (CISO) and a supporting Information Security Analyst in June 2015 and contracted with an external organization to support remediation activities related to information security. On July 30, 2015, the Corporation signed a new Master Information Technology Services (MITS) contract and initiated contractual actions to replace obsolete hardware and software that contributed to noted security weaknesses. Finally, the Corporation established a Memorandum of Agreement (MOA) in November 2014 with DHS to participate in DHS's Continuous Diagnostics and Mitigation (CDM) Program; the Corporation intends to leverage DHS's continuous monitoring services beginning in the second quarter of FY 2016.

While the Corporation is taking a number of important steps to correct previously noted information security weaknesses, these corrective actions were not complete at the close of Kearney's fieldwork. Based on our work performed and evidence gathered through August 30, 2015, we concluded that **the Corporation's Information Security Program and privacy controls were not compliant with respect to FISMA legislation, OMB guidance, and applicable NIST SPs.** In addition to the 10[2] FISMA metric areas, we evaluated privacy controls as a separate area, for a total of 11 areas reviewed. Our testing found **the controls were ineffective in eight of the 11 areas examined. In two of those eight areas, the deficiencies were severe enough to constitute a significant deficiency (i.e., "Continuous Monitoring Management" and "Risk Management").**

[1] CIGIE is an independent entity established within the Executive branch to address integrity, economy, and effectiveness issues that transcend individual Government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the OIG.

[2] Key FISMA metrics identified in the *FY 2015 DHS IG FISMA Metrics* comprise: Continuous Monitoring Management, Configuration Management, Identity and Access Management (IAM), Incident Response and Reporting, Risk Management, Security Training, Plans of Actions and Milestones (POA&M), Remote Access Management, Contingency Planning, and Contractor Systems.

OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, defines a significant deficiency as:

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

Annually, OMB and DHS provide specific instructions and request OIGs to prepare responses to specific information security metric questions. Based on the *DHS FY 2015 IG FISMA Reporting Metrics*, a FISMA evaluation addresses 10 specific aspects of information security, subdivided into 100 individual security metrics. **Of the 100 metrics, our testing identified 54 instances of noncompliance with OMB guidance and NIST SPs. We grouped these instances of noncompliance into 17 findings (four new findings in FY 2015 and 13 repeated findings from prior years).** Of the 13 repeated findings, there are five findings from FY 2013 and eight findings from FY 2014. From the 2014 FISMA report, the Corporation addressed nine recommendations, while 58 recommendations remain open. This report includes 76 recommendations to strengthen the Corporation's Information Security Program. Kearney considers **five[3] of the 17 findings to be high-risk**; following OMB's annual FISMA reporting instructions, we have classified them as significant deficiencies because they require the attention of agency leadership and immediate or near-immediate corrective actions.

Kearney recognizes that the Corporation is operating in an environment of constrained personnel resources and limited funding, while in the midst of modernizing[4] its IT infrastructure and grant application. Resolution of all noted security weaknesses within a single year may be impractical, considering such limitations and other operational priorities. Similar to the FY 2014 FISMA report, Kearney offers the same four broad suggestions to help the Corporation chart an efficient course to achieve reasonable assurance of adequate security:

1. Establish an IT project plan to prioritize and remediate the noted IT security weaknesses, led by the CISO
2. Develop a project plan, inclusive of tasks, milestone dates, and assignments of responsibility
3. Identify the resource skills, associated experience levels, and financial resources necessary for successful implementation of the IT project plan
4. Establish performance metrics for information security with periodic (not less than quarterly)

---

[3] Kearney considers the following five findings to be high-risk: Lack of a Formally Documented and Fully Implemented ISCM Strategy, Multiple Weaknesses with Vulnerability Scanning and Remediation, Organizational Conflict of Interest, Use of an Obsolete and Unsupported Network Monitoring Tool, and Weaknesses with the Corporation's Security Planning and Assessment Process.

[4] OIT IT Modernization's goal is to enhance IT services through improved enterprise services, infrastructure (e.g., delivering IT services, such as hardware, software, network access, e-mail, etc.), mobility, and information security/compliance.

briefings for executive leadership on the metric results and the status of the IT project's efforts to resolve known weaknesses.

Kearney was not engaged to and did not render an opinion on the Corporation's internal controls over financial reporting or financial management systems. Furthermore, the projection of any conclusions based on the findings identified in this report to future periods is subject to the risk that controls may become inadequate because of changes in conditions, the deterioration of compliance with controls, or the introduction of new risk.

For the Corporation's reference, we have included detailed information in a series of appendices. Appendix A: FY 2015 New Findings – Notifications of Findings and Recommendations provides the full text of each new FISMA finding. Appendix B: Status of Prior Year Findings reviews the status of findings and recommendations from prior years. Appendix C: Management's Response provides the Corporation's response to the draft FISMA report. Appendix D: Kearney and OIG Comments on Planned Actions indicates whether the Corporation's planned actions are responsive to noted weaknesses and recommendations. Appendix E: Responses to *DHS FY 2015 Inspector General FISMA Reporting Metrics* contains responses to each of DHS's 100 security metrics. Appendix F: Results from Field Office Assessments contains results of the Corporation's site assessments.

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

Sincerely,

Kearney & Company, P.C.
November 13, 2015

2. BACKGROUND

2.1 Corporation Overview

The Corporation for National and Community Service (the Corporation) was established in 1993 to connect Americans of all ages and backgrounds with opportunities to give back to their communities and the 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 approximately 650 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 necessary to carry out the mission of the Corporation.

2.2 Information Technology Overview

The Corporation relies on information technology (IT) systems to accomplish its mission of cost-effectively providing and managing volunteer services nationally; it strives to deliver excellent customer service at the lowest cost without sacrificing service levels or quality or disrupting/ degrading any services. The Corporation has an inventory of 11 information systems. The Federal Information Processing Standard (FIPS) Publication (PUB) 199[5] security categorization levels of these systems are moderate (nine of 11 systems) and low (two of 11 systems). Of the 11 information systems, 10 are hosted and operated by third-party service providers. The Corporation's network consists of multiple sites: Headquarters, one Field Financial Management Center (FFMC), five National Civilian Community Corps (NCCC) campuses, one Volunteers in Service to America (VISTA) Member Support Unit (VMSU), and many state offices in cities throughout the United States. These sites are connected with high-speed network connections.

Sustaining high levels of service at low costs is challenging for the Corporation. The Corporation determined that outsourcing its IT infrastructure, while simultaneously implementing changes in IT governance, would provide the highest quality systems at the lowest cost. Outsourcing is not inherently detrimental to the security posture of the organization, but it tends to introduce different considerations and new risks regarding the protection of information and information systems. While the Corporation elected to outsource a significant share of IT functions, it retains responsibility, by law, for complying with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) and security control implementation.

[5] The security categories (i.e., low, moderate, and high) are based on the potential impact on an organization, should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Consequently, the Corporation sought contractors to manage its three primary information systems:

1. General Support System (GSS) – Delivery of application and system hosting, processing, and network services to support the Corporation's mission through the Managed Data Center Services (MDCS) contract, which was subsequently replaced with Managed Information Technology Services (MITS) contract. This includes:
   - Data center services, such as server services, middleware administration and support, system-level database administration and support, storage services, and custodian of software licenses
   - Data network and security services, such as network managed services, secure point-to-point communications within the network, secure hosting environment, and IT components that comply with applicable Federal security and privacy mandates
   - Cross-functional services, such as: planning, analysis, requirements definition; engineering; facility and environmental infrastructure; operations, administration, and maintenance of infrastructure; and IT Infrastructure Library (ITIL)-based service management processes
2. Electronic-System for Programs, Agreements, and National Service Participants (eSPAN) – Custom web application based on an Oracle database for the National Service Trust (TRUST) and participant systems. eSPAN tracks AmeriCorps members and TRUST educational awards, including awards made to all individuals in the 20-year history of the Corporation (approximately 1.2 million individuals)
3. Momentum Financial Management System (Momentum) –Multi-tier, distributed, commercial off-the-shelf (COTS) enterprise financial management software system supporting data exchange with other Federal systems, providing financial planning capabilities and a means to record the agency's financial transactions. Momentum is the official system of record for financial management at the Corporation and records financial planning, purchasing, accounts receivable, accounts payable, disbursements (to include payroll), and other budget activities, which are integrated so that transactions update budgets, financial plans, and the general ledger when processed.

2.3 FISMA

FISMA Legislation

The Federal Information Security Management Act of 2002 (FISMA-2002) was enacted into United States Federal law under Title III of the E-Government Act of 2002, Public Law (P.L.) 107-347 (December 17, 2002), 44 United States Code (U.S.C.) §§ 3541-49. The Federal Information Security Modernization Act of 2014 (FISMA) was enacted into United States Federal law as P.L. 113-283 (December 18, 2014), 44 U.S.C. §§ 3551-58. FISMA replaced the portion of FISMA-2002 codified in 44 U.S.C. Chapter 35, Subchapters II and III, but left other portions in effect.

Unless otherwise noted, references to FISMA in this report refer to the 2014 legislation.

FISMA was amended in 2014 to delineate the roles and responsibilities of the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS), move agencies away from paperwork-heavy processes and towards real-time automated security, and place greater management and oversight attention on data breaches.

FISMA outlines the information security management mandates for agencies, including the requirement for an annual evaluation by each agency's Inspector General (IG) or an independent external auditor. The results of the evaluation must be reported to OMB and Congress, utilizing an automated reporting tool, CyberScope, no later than November 15 of each year.

While the 2014 version of FISMA retains the FISMA-2002 requirement for the Office of Inspector General (OIG) to conduct an annual evaluation of the agency's Information Security Program, the focus has changed. Instead of evaluating the agency's **compliance** with information security policies, procedures, standards, and guidelines, the updated FISMA requires an assessment of the **effectiveness** of those information security policies, procedures, standards, and guidelines.

Key requirements of FISMA legislation include:

- The development, documentation, and implementation of an agency-wide Information Security Program to provide 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 to determine the effectiveness of such program and practices, to include:
  - Testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems
  - An assessment of the effectiveness of the information security policies, procedures, and practices of the agency.

The statute also imposes minimum standards for agency information systems. FISMA requires Federal agencies to implement the following information security practices:

- Provision of information security protection commensurate with the risk and magnitude of harm resulting from compromise of information or information systems maintained by or on behalf of the agency
- Compliance with information security policies, procedures, standards, and guidelines issued by OMB and DHS under the authority of FISMA
- Delegation of authority to the Chief Information Officer (CIO) to ensure the design and implementation of information security policies are consistent with OMB and the National Institute of Standards and Technology (NIST) guidance
- Security awareness training programs
- Periodic testing and evaluation of the effectiveness of security policies, procedures, and practices to be performed with a frequency depending on risk, but no less than annually
- Periodic risk assessments

- Processes to manage remedial actions for addressing deficiencies
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations for information systems
- Annual reporting on the adequacy and effectiveness of the Information Security Program to OMB, the Secretary of DHS, and Congress.

OMB is responsible for reporting a summary of the results of an agency's compliance with FISMA requirements to Congress. OMB's 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 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 for addressing recommendations identified as a result of findings from security control assessments, security impact analyses, continuous monitoring activities, and other assessments. OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*, provides a roadmap for ensuring continuous agency security improvement and formally assisting agency officials with prioritizing corrective action and resource allocation.

2.3.1 NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to Federal information systems. These include information security standards that establish minimum information security requirements necessary to improve the security of Federal information and information systems. FISMA also requires that Federal agencies comply with FIPS issued by NIST. In addition, NIST develops and issues Special Publications (SP) as recommendations and guidance documents.

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates the use of NIST SP 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, to provide guidelines for selecting and specifying security and privacy controls for information systems supporting an agency to meet the requirements of FIPS PUB 200. NIST SP 800-53, Rev. 4 organizes the security controls into 18 families, and each security control family includes security controls associated with the security functionality of the family. The NIST SP 800-53, Rev. 4 security control families are shown in ***Exhibit 1***.

Exhibit 1: Security Control Families

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

The Corporation's information systems are categorized according to FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, and NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. The system categorization process starts with the determination of the importance of an information system to the agency mission and the impact on loss of confidentiality, integrity, and availability of the information system and data to the agency's operations, assets, or individuals. Based on the FIPS PUB 199 standard, all Corporation systems are categorized as having a moderate or low security impact.

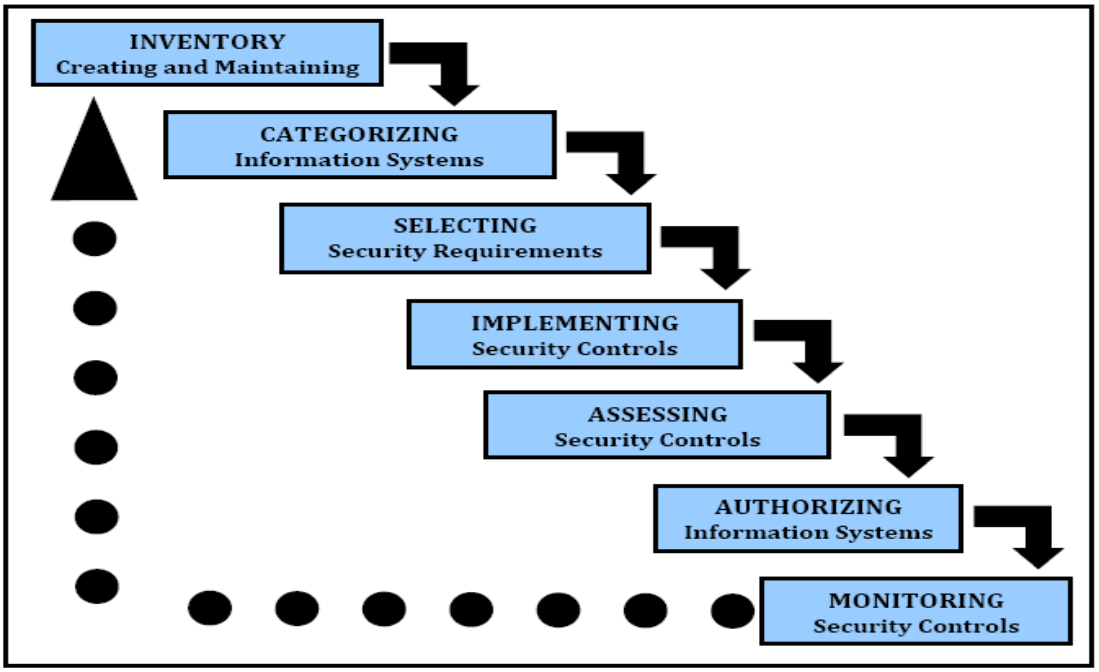
The Corporation has adopted guidance from NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, for authorizing its systems. The NIST Risk Management Framework (RMF) comprises the following six steps and provides a structured practice for incorporating information security and risk management activities into the system development lifecycle (SDLC):

1. **Categorize** the information system and the information processed, stored, and transmitted by that system based on an impact analysis
2. **Select** an initial set of baseline security controls for the information system based on the security categorization and then tailor and supplement the security control baseline, as needed, based on an organizational assessment of risk and local conditions
3. **Implement** the security controls and describe how the controls are employed within the information system and its environment of operation

4. **Assess** 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
5. **Authorize** information system operations 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
6. **Monitor** the security controls in the information system on an ongoing basis, to include 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.

To implement the NIST RMF, agencies must maintain an inventory of their information systems, as required by FISMA. Incorporating this prerequisite of maintaining an inventory of information systems, Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") developed the diagram, shown in ***Exhibit 2***, to reflect the "waterfall" nature of the NIST RMF.

Exhibit 2: NIST RMF



Source: Kearney Analysis of NIST SP 800-37, Rev. 1

2.3.2 DHS 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 the OIG to prepare its annual responses using CyberScope, DHS provides instructions in the *FY 2015 IG FISMA Reporting Metrics* and

requires each agency OIG to respond to 100 FISMA metric questions in 10 metric areas. Appendix E: Responses to *DHS's FY 2015 IG FISMA Reporting Metrics* contains the OIG's responses for the Corporation. ***Exhibit 3: Summary of FY 2015 DHS IG FISMA Responses*** in Section 3 lists the 10 FISMA metric areas and provides Kearney's test results.

2.4 Scope

Kearney conducted an independent evaluation of the Corporation's Information Security Program from May through August 2015. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation* promulgated by CIGIE and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

In order to assess how the Corporation established its agency-wide Information Security Program and practices as required by FISMA, Kearney performed detailed testing of the Corporation's GSS and two major applications, eSPAN and Momentum, for compliance with selected NIST SP 800-53, Rev. 4 controls. In addition to the 10 FISMA metric questions, Kearney tested the Corporation's privacy controls.

The FISMA evaluation included an assessment of the following:

- Site visits to two Corporation State Offices (Maryland and Pennsylvania), the NCCC Atlantic Region in Baltimore, and the FFMC in Philadelphia
- The Corporation's Information Security Program and privacy controls
- Management oversight of contractor-managed systems, including the Corporation's network and My AmeriCorps Portal.

3. RESULTS

From our testing, we found that **the Corporation was noncompliant with the FISMA legislation, OMB guidance, and NIST SPs in 54 of 100 security metric areas**. Addressing these deficient security practices will strengthen the Corporation's Information Security Program and contribute to ongoing efforts to achieve reasonable assurance of adequate security over information resources.

This section provides the conclusions of our research, analysis, and assessment of the Corporation's Information Security Program, policies, and practices and privacy controls. Kearney cites authoritative policies, standards, and guidance, where applicable. As ***Exhibit 3*** illustrates, eight of the 11 areas evaluated warrant additional management attention to address identified deficiencies. Kearney concluded that the Corporation's privacy controls also require management attention to address identified deficiencies. To determine the severity of noted exceptions, Kearney considered guidance from the Government Accountability Office's (GAO) Generally Accepted Government Auditing Standards (GAGAS) and OMB's Memorandum M-14-04 definition of a significant deficiency, and we applied professional judgment. The following sections summarize the results of our testing organized by the 10 FISMA metric areas.

Kearney's proposed responses to the *DHS IG FISMA Metric* questions are contained in Appendix E and are cross-referenced to the associated findings in this section.

Exhibit 3: Summary of FY 2015 DHS IG FISMA Responses/Comparison to FY 2014 Results

2015 DHS IG FISMA Reporting Area	**2014:** # of DHS Exceptions/ Total DHS IG Security Metric Questions	FY 2014 - Severity of Noted Exceptions	**2015:** # of DHS Exceptions/ Total DHS IG Security Metric Questions	FY 2015 - Severity of Noted Exceptions	Controls Effective Overall (Yes/No)
1. Continuous Monitoring Management	8 of 8	Significant Deficiency	8 of 8[6]	Significant Deficiency	No
2. Configuration Management	7 of 13	Control Deficiency	9 of 12	Control Deficiency	No
3. Identity and Access Management	1 of 12	Control Deficiency	1 of 9	Control Deficiency	Yes
4. Incident Response and Reporting	2 of 9	Control Deficiency	2 of 8	Control Deficiency	Yes
5. Risk Management	10 of 17	Significant Deficiency	9 of 16	Significant Deficiency	No
6. Security Training	2 of 7	Control Deficiency	3 of 7	Control Deficiency	No
7. Plans of Action and Milestones (POA&M)	6 of 9	Significant Deficiency	6 of 9	Control Deficiency	No
8. Remote Access Management	1 of 13	Control Deficiency	3 of 12	Control Deficiency	Yes
9. Contingency Planning	8 of 13	Control Deficiency	10 of 12	Control Deficiency	No
10. Contractor Systems	4 of 8	Control Deficiency	3 of 7	Control Deficiency	No
†Privacy	N/A	Significant Deficiency	N/A	Control Deficiency	No
Total	49 of 109	4 Significant Deficiencies, 7 Control Deficiencies	54 of 100	2 Significant Deficiencies, 9 Control Deficiencies	No

[6] To enable comparison of this year's results with those of FY 2014, Kearney analyzed this year's Continuous Monitoring Management using the same eight Continuous Monitoring Management questions applicable in FY 2014. However, a new standard for assessing Continuous Monitoring Management, using a maturity model, went into effect on June 19, 2015, and Kearney assessed the Corporation's Continuous Monitoring Management under that standard. As we discuss below, the maturity model yields the Corporation a score of "1 – Ad Hoc" in each of the three areas (People, Process, and Technology) scored.

2015 DHS IG FISMA Reporting Area	**2014:** # of DHS Exceptions/ Total DHS IG Security Metric Questions	FY 2014 - Severity of Noted Exceptions	**2015:** # of DHS Exceptions/ Total DHS IG Security Metric Questions	FY 2015 - Severity of Noted Exceptions	Controls Effective Overall (Yes/No)
Legend: † – Consistent with the addition of privacy controls to NIST SP 800-53, Rev. 4, the OIG contracted with Kearney to evaluate the Corporation's implementation of specific privacy controls as part of the FY 2015 FISMA evaluation.					

Kearney's testing resulted in 17 Notifications of Findings and Recommendations (NFR). Four of the 17 findings are new and described in Appendix A, while 13 of the 17 findings were repeated or updated from the FY 2014 FISMA evaluation, as described in Appendix B. The Corporation implemented nine of 67 recommendations from the FY 2014 FISMA evaluation, while 58 recommendations from prior year remain open and are repeated; additionally, three new recommendations were added to address FY 2014 findings. **In most instances, the Corporation has taken some corrective actions to address the remaining 58 outstanding recommendations.** In addition, Kearney identified **four new security weaknesses in the FY 2015 FISMA evaluation and made 15 additional recommendations**. Results from Kearney's FY 2015 FISMA evaluation are summarized below:

Continuous Monitoring Management

1. *Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring Strategy (Repeat finding from FY 2013 and FY 2014 FISMA evaluation) (FY 2014 FISMA Finding #1)*

   Severity: Significant Deficiency

   On May 27, 2015, CIGIE released a new model for evaluating Continuous Monitoring Management. Whereas the prior approach focused on compliance with specific OMB- and NIST-mandated security standards, the new model centers on the maturity and effectiveness of Federal agencies' Information Security Continuous Monitoring (ISCM) capabilities and practices. CIGIE and OMB expect to extend a similar maturity and effectiveness approach to other FISMA performance metric areas in the near future. Using this maturity model, on a scale of 1-5, the Corporation received a "1 – Ad-Hoc" maturity for each of the three evaluation areas (i.e., People, Process, and Technology) as of August 30, 2015.

   The Corporation has not formally documented and implemented an organization-wide ISCM Program and strategy. As part of monitoring its outsourced information systems, the Corporation has not developed meaningful and reportable performance metrics to evaluate the IT contractors' performance and incorporated such performance metrics into its IT contracts. An ISCM strategy is a critical first step in identifying and rectifying these and other gaps to ensure that sensitive systems and information remain secure.

2. *Multiple Weaknesses with Vulnerability Scanning and Remediation (FY 2014 FISMA Finding #2)*

Severity: Significant Deficiency
The Corporation has taken some steps, but with limited progress, to resolve the prior year weaknesses. The Corporation has indicated its intent to replace its current vulnerability scanning tool as part of the technology refresh with a new tool that more effectively identifies missing application security patches and provides better reporting. Kearney identified four deficiencies related to vulnerability scanning and the remediation process at the Corporation. Specifically, the Corporation did not:

a. Use a vulnerability scanning tool that complied with NIST vulnerability standards and supported the Security Content Automation Protocol (SCAP)
b. Scan desktops and laptops on a monthly basis for missing security patches and/or configuration errors
c. Periodically perform a scan for configuration errors and deviations from the United States Government Configuration Baseline (USGCB)[7] for desktops
d. Include performance metrics for the timely remediation of identified vulnerabilities in the new MITS contract.

3. *Inadequate Planning and Untimely Award of IT Contract Delays Remediation of Information Security Weaknesses (FY 2015 FISMA Finding #1)*

Severity: Control Deficiency
The Corporation did not timely replace the MDCS contract upon its expiration. Instead, the MDCS contract was repeatedly extended for a total of eight months, allowing multiple high-risk security vulnerabilities identified in prior FISMA evaluations to persist.

4. *Outdated IT Strategic Plan and Lack of Enterprise Architecture Plan (FY 2015 FISMA Finding #3)*

Severity: Control Deficiency
The Corporation has not formally documented its IT strategy and enterprise architecture plan. The Corporation's IT strategic plan did not contain all of the IT modernization[8] plans, and the Corporation does not have an enterprise architecture plan to ensure chosen solutions would meet the Corporation's long-term needs.

[7] USGCB is a secure configuration standard for Windows XP, Vista, and Windows 7 desktop that specifies over 550 secure settings that NIST maintains and updates in response to new security vulnerabilities. The large number of security settings means that manual review is impractical without the use of an automated tool that supports the SCAP protocol.
[8] The Office of Information Technology (OIT) IT Modernization's goal is to enhance IT services through improved enterprise services, infrastructure (e.g., delivering IT services, such as hardware, software, network access, e-mail, etc.), mobility, and information security/compliance.

5. *Organizational Conflict of Interest (FY 2014 FISMA Finding #3)*

Severity: Significant Deficiency
NIST SP 800-53 requires that security assessors be independent and impartial when performing security assessments for FIPS PUB 199-rated moderate and high-impact information systems. The Corporation permitted its MDCS contractor to perform the Security Assessment and Authorization (SA&A) of the Corporation's GSS and eSPAN information systems, rather than requiring that the MDCS contractor hire an independent party. The security assessors, who had primary responsibility for monitoring the Corporation's network, worked for the MDCS contractor and reported to the overall Project Manager. The security assessors were effectively reviewing their own work and that of their colleagues; their employment status, assigned job responsibilities, and organizational reporting relationships precluded an impartial and objective evaluation of security controls.

The Corporation has taken steps to resolve this prior year weakness by hiring an independent Information Assurance Program Support (IAPS) contractor in May 2015 to perform a review and validation of security assessments. However, the IAPS contractor had not completed any independent security assessments as of August 2015. During the period of October 1, 2014 to July 31, 2015, the MCDS contractor staff, rather than an independent party, performed the required security control assessments. The Corporation indicated that the IAPS contractor would assume these responsibilities in future years.

6. *Use of an Obsolete and Unsupported Network Monitoring Tool (FY 2014 FISMA Finding #4)*

Severity: Significant Deficiency
The Corporation's primary tool for network monitoring and audit log analysis is obsolete and unsupported by the vendor. Additionally:

a. The Corporation did not have a standard operating procedure (SOP) requiring the periodic review and maintenance of the primary network monitoring and audit log tool, which had not been reviewed and tuned for the audit alerts in more than two years
b. The monitoring tool did not retain audit events for long enough to allow useful aggregation to identify trends and perform targeted analysis
c. The Corporation had not established performance metrics to increase accountability for network and audit log monitoring and improve effectiveness of information security.

The Corporation has indicated its intent to replace the network tool as part of the new MITS contract and utilize its Security Information and Event Management (SIEM) solution.

Configuration Management

7. *Risks to the Confidentiality and Availability of Voice Communications (FY 2014 FISMA Finding #6)*

   Severity: Control Deficiency
   The Corporation does not separate its data network traffic from its voice network traffic. Specifically, Corporation desktops were able to ping (query) Cisco Voice over Internet Protocol (VoIP) phones at remote offices. In addition, users were able to access the Cisco VoIP phones using their desktops' web browser over hypertext transfer protocol (HTTP). The connectivity between the data and voice virtual local area networks (VLAN)[9] could be exploited by malicious individuals to compromise VoIP components, which generally were not designed with security in mind and could allow an attacker to intercept and record phone calls. The Corporation reports that it has deferred action to resolve this prior year weakness pending its planned relocation in FY 2016.

Identity and Access Management (IAM)

8. *Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement (FY 2015 FISMA Finding #2)*

   Severity: Control Deficiency
   The Corporation's manual process for granting and terminating user account access was not effective at identifying accounts that are inactive or assigned to employees or contractors no longer associated with the Corporation. Subsequent to Kearney's testing, the Corporation implemented a new system for account management of new, modified, and separated users.

Risk Management

9. *Inadequate Enterprise-Wide Risk Management Policies and Practices (Repeat finding from FY 2013 FISMA evaluation) (FY 2014 FISMA Finding #9)*

   Severity: Control Deficiency
   The Corporation's documented risk management policies and security controls described the risk management process at the information system (Tier 3) level but do not address risks at Tier 1 (Organization) and Tier 2 (Mission/Business). The risk management practices largely do not involve the individuals who are responsible for

[9] According to Cisco, a VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire when, in fact, they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

accomplishing organizational, mission, and business objectives on a daily basis, such as the business owner or application owner. The Corporation has made improvements in risk management and has documented, in draft format, three levels of management to cover the enterprise level (Tier 1), the missions/business level (Tier 2), and the information systems level (Tier 3). However, the Corporation has not conducted a Business Impact Analysis (BIA) to identify mission-critical business functions and quantify the impact of a loss of those functions.

10. *Weaknesses with the Corporation's Security Planning and Assessment Process (Repeat finding from FY 2013 FISMA evaluation) (FY 2014 FISMA Finding #10)*

Severity: Significant Deficiency
The Corporation did not develop corporate standards for its multiple IT contractors to follow regarding ongoing security assessments and continuous monitoring activities. Kearney's testing of IT security controls across a multitude of the Corporation's information systems identified multiple inconsistencies and inaccuracies in the System Security Plans (SSP), Security Assessment Report (SAR), and POA&Ms, highlighting the inconsistent nature, depth, and quality of security assessments and continuous monitoring activities performed by the Corporation's IT vendors.

While the Corporation has provided some high-level guidance, it did not provide detailed instructions to ensure consistency and compliance with NIST guidance when conducting security assessments. Specifically, the Corporation:

a. Has not developed standard test cases
b. Has not developed a sampling plan for testing
c. Has not documented its approach for testing common controls or how required security controls that are not within the scope of the IT service provider's information systems are assessed
d. Has not specified when security assessor independence and impartiality is required and when it may be waived
e. Did not require its security control assessors to compare the implementation details from the SSP to actual practice and note any discrepancies
f. Did not use establish templates for Acceptance of Risk for all identified and accepted risks.

11. *Inaccurate Inventory of Physical IT Assets (FY 2015 FISMA Finding #4)*

Severity: Control Deficiency
The Corporation did not effectively implement its IT inventory management procedures. Kearney visited four sites and noted that none of the sites had an accurate inventory of physical IT assets maintained onsite and that some physical IT assets that were onsite were not listed on the inventory spreadsheet.

Security Training

12. *Lack of Formal, Role-Based Training (Repeat finding from FY2013 FISMA evaluation) (FY 2014 FISMA Finding #11)*

Severity: Control Deficiency
The Corporation has not implemented a formal, documented, role-based Information Security Training Program that includes regular training updates.

POA&Ms

13. *Improvements Needed to POA&M Reporting (Repeat finding from FY2013 FISMA evaluation) (FY 2014 FISMA Finding #12)*

Severity: Control Deficiency
The Corporation's POA&Ms did not identify resources required to resolve open tasks, such as estimating the level of effort in hours or other costs to procure contractor support or tools. Additionally, none of the 60 open POA&M items specified the resources required for issue resolution, and 56 of the 60 items listed on the Corporation's May 2015 POA&M lacked a scheduled remediation date. Finally, the Corporation did not document its acceptance of risk for items that it chose not to remediate or indicate any planned mitigating controls.

For FY 2015, the Corporation made progress by establishing an entity-level POA&M. Nevertheless, weaknesses remain, including failure to ensure that all POA&M items have due dates, an individual assigned responsibility for remediation, and an estimated level of effort or cost to resolve the noted weakness.

Remote Access Management

14. *Inadequate Controls over Remote Access (FY 2014 FISMA Finding #13)*

Severity: Control Deficiency
Corporation-issued laptops were configured to connect automatically to the Corporation's network through Cisco's "AnyConnect VPN" client. However, the automatic connection of the laptop to the Virtual Private Network (VPN) server does not meet the two-factor authentication requirements for Federal agencies where "one of the factors is provided by a device separate from the computer gaining access."[10] The Corporation's current VPN solution authenticates remote devices using a single factor, a shared digital certificate common to all corporate laptops, rather than second factor such as a RSA token, which is physically separate and unique from the device gaining access. In addition, the Corporation incorrectly configured its VPN to permit

[10] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006.

the use of noncompliant, FIPS[11] encryption protocols,[12] leaving VPN sessions vulnerable to exploitation, such as "man-in-the-middle attacks." Specifically, the Corporation's VPN device used for connectivity only supports TLS 1.0. NIST SP 800-52, Rev. 1, Section 3, "Minimum Requirements for TLS Servers," Subsection 3.1, *Protocol Version Support*, states, "TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. The use of TLS version 1.2 is strongly recommended." Corporation oversight of the VPN deployment did not identify the use of non-approved FIPS-140-2 protocols or that the Corporation's deployed VPN connection device only supports TLS 1.0.

Contingency Planning

15. *Inadequate Disaster Recovery Plan Documentation and Planning (FY 2014 FISMA Finding #14)*

Severity: Control Deficiency
The Corporation's Disaster Recovery documentation does not plan for reconstitution of all of the Corporation's essential functions and missions in the event of a disaster. In fact, the BIA[13] specifically states that it is not meant to address all essential business functions and refers to the Continuity of Operations Plan (COOP) and the Corporation Disaster Recovery Plan (DRP) for coverage. However, the COOP and DRP do not identify all essential business functions. Further, the Corporation's DRP was specifically created for the MITS contract and is not representative of the Corporation as a whole.

16. *Lack of Adequate Testing of COOP (FY 2014 FISMA Finding #15)*

Severity: Control Deficiency
The Corporation has not conducted adequate planning or testing of its COOP. The following aspects of the Corporation's COOP and DRP make it inadequate:

a. The COOP does not include sufficient information to address all mission-essential functions and subordinate plans and details that would be necessary should the plan ever need to be activated
b. The Corporation has made assumptions that do not appear reasonable should it be necessary to activate the COOP, such as electronic availability of all vital records and availability of laptops to all employees supporting essential business functions
c. There is no evidence that the agency conducted annual COOP testing, including after-action reports, as required for mission-essential functions and the agency's

[11] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.*
[12] RC4, SSL 3.0, and SSL 3.1/TLS 1.0. RC4, SSL 3.0, and TLS 1.0 are widely used commercially, but have several technical flaws that can increase the risk of exploitation and are not FIPS 140-2-approved.
[13] BIA is systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, or emergency.

financial system.

Privacy

17. *Inadequate Controls over Privacy (FY 2014 FISMA Finding #16)*

Severity: Control Deficiency
The Corporation demonstrated multiple weaknesses in the implementation of privacy controls, including:

a. The Corporation has not fully documented its personally identifiable information (PII) inventory
b. Corporation employees did not comply with requirements to destroy outdated records containing PII in accordance with the applicable Record Retention Schedule, promulgated by the National Archives and Records Administration (NARA)
c. The Corporation did not update Privacy Impact Assessments (PIA) for two key information systems, Momentum and eSPAN, since 2009 and did not publicly post the PIAs on the Corporation's website.

Implications of Relying on Contractor Systems

The election to outsource significant IT functions does not relieve the Corporation of its responsibility to comply with the requirements of FISMA and security control implementation. Instead, the Corporation assumes the obligation to assure that the contractor meets the applicable standards. Because the Corporation has chosen to outsource nearly all of the relevant systems and functions, we have reported issues arising from contractor systems under the specific FISMA metric area, rather than aggregating them as contractor issues. In the majority of these cases, the Corporation did not exercise sufficient oversight of critical contractor functions.

APPENDIX A: FY 2015 NEW FINDINGS – NOTIFICATIONS OF FINDINGS AND RECOMMENDATIONS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") issued 17 Notifications of Findings and Recommendations (NFR) to the Corporation for National and Community Service (the Corporation) as a result of the fiscal year (FY) 2015 Federal Information Security Modernization Act of 2014 (FISMA) Independent Evaluation. Appendix A describes the four new NFRs.

1. Continuous Monitoring

Finding #1: Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses (*See Appendix E, DHS Question # 1: Continuous Monitoring Management)*

Background: The Corporation relies extensively on information technology (IT) systems to fulfill its mission and has implemented an outsourcing strategy to achieve higher quality at lower costs. Reliance on outsourcing affects the implementation of required information security controls. Outsourcing is not inherently detrimental to the security posture of an organization, but it does introduce different considerations and new risks regarding the protection of information and information systems. Thus, it is essential that contracts for IT services include applicable information security requirements and performance metrics indicative of security. Clear performance metrics must be detailed thoroughly in IT contracts to enable service providers to understand fully the requirements, regulations, and performance metrics that they will be subject to under the awarded contract or task order.

In the FY 2014 FISMA evaluation, Kearney identified 49 information security weaknesses and aggregated them into 16 NFRs.[14] Five NFRs involved the Corporation's Managed Data Center Services (MDCS) provider, and four of them were so serious as to be designated "Significant Deficiencies."[15] These findings are as follows:

- Finding #2: Multiple Weaknesses with Vulnerability Scanning and Remediation (Significant Deficiency)
- Finding #3: Organizational Conflict of Interest (Significant Deficiency)
- Finding #4: Use of an Obsolete and Unsupported Network Tool (Significant Deficiency)

[14] Full text of the FY 2014 Corporation OIG FISMA evaluation is available online at http://www.cncsoig.gov/sites/default/files/15-03_0.pdf.

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

- Finding #10: Weaknesses with the Corporation's Security Planning and Assessment Process (Significant Deficiency)
- Finding #11: Lack of Formal Role-Based Training (Control Deficiency).[16]

These security control weaknesses resulted from a combination of three common causes:

1. The Corporation's oversight of the MDCS contract was deficient
2. MDCS contractual clauses pertaining to information security were not enforced
3. The MDCS contract did not clearly define outcomes and measures of performance related to information security.

The Corporation's management indicated that it intended to correct many of the security weaknesses identified in the FY 2013 and FY 2014 FISMA evaluations by replacing the MDCS contract upon its expiration in November 2014 with a new contract vehicle containing appropriate new security requirements. Examples included requiring the new vendor to replace obsolete and unsupported network tools in a timely manner, performing monthly vulnerability scans, remediating identified weaknesses on servers, and maintaining a list of known security weaknesses, also known as a Plan of Action and Milestones (POA&M). Such operational activities are good candidates for service-level agreements (SLA) and specific measures of performance.

Condition: The Corporation did not timely replace the MDCS contract upon its expiration. Instead, the MDCS contract was repeatedly extended for a total of eight months, allowing multiple high-risk security vulnerabilities identified in prior FISMA evaluations to persist.

Moreover, notwithstanding recommendations in the FY 2014 FISMA evaluation that any new IT contract specify the level of services to be provided and include performance metrics relative to information security, these critical elements were omitted from the base/Master Information Technology Services (MITS) contract. Thus, these elements are not included in the predetermined cost, and the Corporation may be required to pay extra to achieve basic levels of information security.

From interviews with the Office of Procurement Service (OPS) and the Office of Information Technology (OIT), Kearney prepared the following timeline to highlight the procurement process and provide context for the multiple delays:

Date	Contractual Event
12/2013	The Corporation determines it needs third-party assistance to develop a Statement of Work (SOW) for replacement contract for the MDCS contract (to be called MITS).

[16] OMB A-123, *Management's Responsibility for Internal Control*, states, "A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis."

Date	Contractual Event
2/18/2014	A non-profit research company, MITRE, provides the proposal to develop an SOW for the Corporation.
06/2014	The Corporation awards a sole-source contract to develop the SOW for the MITS contract to MITRE.
11/30/2014	The MDCS contract expires. OPS awards a six-month contract extension to May 31, 2015.
12/31/2014	The Corporation receives an SOW from MITRE.
02/27/2015	The Corporation posts the solicitation for the MITS contract.
04/28/2015	The Corporation receives two proposals from bidders.
05/31/2015	The six-month extension to the MDCS contract expires. The Corporation awards a sole-source, one-month contract to the MDCS incumbent with five one-month option periods.
06/30/2015	The Corporation awards first option of sole-source contract through July 31, 2015.
08/01/2015	After 93 days of internal review, the Corporation awards the MITS contract to the MDCS incumbent. The Blanket Purchase Agreement (BPA) lasts seven years and has a contract ceiling of $50 million.

Sources: OPS interview on September 1, 2015 and OIT discussions on August 24, 2015 and September 2, 2015.

As noted above, the Corporation received only two proposals for the seven-year IT services BPA worth potentially $50 million. According to OPS, one bid was not credible; thus, the Corporation selected the incumbent MDCS contractor. In light of the limited competition for the BPA, the Corporation did not re-issue the solicitation to receive additional bids or inquire of invited bidders why the Corporation received a limited response for such a large procurement.

Criteria: OMB Circular A-50, *Audit Followup*, requires agency officials to initiate timely corrective actions in response to noted weaknesses. Furthermore, OMB encourages prompt resolution when the severity of the noted control weakness rises to a "Significant Deficiency."

OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, asserts that agencies are responsible for ensuring IT acquisitions comply with the IT security requirements in FISMA (44 U.S.C. 3544), Appendix III of OMB Circular A-130, and guidance and standards from the National Institute of Standards and Technology (NIST). NIST has released several publications that focus on procurement of IT systems:

- NIST Special Publication (SP) 800-35, *Guide to Information Technology Security Services*
- NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*
- NIST SP 800-36, *Guide to Selecting Information Technology Security Products*
- NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*.

Regarding the limited competition for the MITS procurement, the Federal Acquisition Regulation (FAR) requires agencies to take steps to promote full and open competition. The FAR states:

> **"Subpart 6.1-Full and Open Competition**
> **6.100 Scope of subpart.** This subpart prescribes the policy and procedures that are to be used to promote and provide for full and open competition.
> **6.101 Policy.**
> (a) 10 U.S.C. 2304 and 41 U.S.C. 3301 require, with certain limited exceptions (see subpart 6.2 and 6.3), that contracting officers shall promote and provide for full and open competition in soliciting offers and awarding Government contracts.
> (b) Contracting officers shall provide for full and open competition through use of the competitive procedure(s) contained in this subpart that are best suited to the circumstances of the contract action and consistent with the need to fulfill the Government's requirements efficiently (10 U.S.C. 2304 and 41 U.S.C. 3301)."

Cause: The Corporation did not adequately plan and manage the solicitation and procurement process to allow a timely award of a new contract that included necessary information security elements. Kearney met with both OPS and OIT to understand the factors that resulted in the untimely contract award and omission of SLAs and measures of performance related to information security. OPS attributed the delays awarding the contract to employee turnover within OPS, a poorly written SOW that required multiple revisions, an inexperienced source selection panel, and a poorly written Source Selection Determination Memorandum that required multiple revisions. OIT attributed the delays to poor contract performance by the selected non-profit research firm[17] and unclear evaluation instructions from OPS that resulted in multiple rewrites of the Source Selection Determination Memorandum. Regarding the lack of SLAs and measures of performance, OPS indicated that MITRE did not review the FY 2013 or 2014 Office of Inspector General (OIG) FISMA evaluation reports during the SOW development. The Corporation paid more than $300,000 for the development of requirements and preparation of an SOW that failed to consider the key weaknesses in information security or to leverage the extensive work directed to those issues. Neither OIT nor OPS identified the omission of OIG FISMA recommendations in their review of the SOW.

From interviews with OPS and OIT, Kearney observed that the procurement process is largely managed informally using Corporate e-mail, rather than a centralized, procurement management system that tracks workflow and due dates against a procurement schedule. Kearney requested, but did not receive, evidence that the Corporation routinely reports the status of significant procurements against an established procurement timeline to the Corporation's executive leadership to highlight delays and possible need for executive involvement. Further, Kearney observed that the procurement process does not require Contracting Officer's Representatives (COR) to complete Contractor Performance Assessment Reporting System (CPARS) reviews at

[17] According to OPS, the non-profit research firm, MITRE, missed internal milestone dates to deliver an acceptable SOW and required a contract extension to complete the task.

the completion of a contract to highlight whether the contractor received a "cure" notice or was subject to any OIG audits or investigations during the period of performance. In both cases regarding MITRE and the prior MDCS contractor, the Corporation did not complete CPAR evaluations to highlight contract performance concerns.

Regarding the limited responses from the IT vendor community, the Corporation does not know why it received only two proposals, despite allowing for a 60-day response window and distributing the SOW to approximately 20 IT vendors. While not explicitly required by law or OMB guidance, Kearney observed that the Corporation did not follow many common practices associated with large IT procurements. For example, many Federal agencies frequently distribute draft SOWs to potential IT vendors on large, multi-year BPAs with the intention of receiving industry comments. Other common practices include marketing the SOW to potential bidders by hosting an industry day and contacting potential bidders to inquire whether they intend to bid based on the draft SOW. Upon receipt of only two proposals, OPS did not contact organizations that received the SOW, but chose not to bid to understand the organizations' reasons for not bidding. If industry feedback suggested that the SOW contained ambiguous or unreasonable requirements that prevented sufficient competition, procurement officials could have revised and re-issued the SOW to increase competition. However, according to OPS officials in a September 1, 2015 interview, they did not take any of the above actions.

Effect: Two serious flaws compromised the award of the replacement contract, by which the Corporation intended to remedy prior security weaknesses. First, the untimely award of the MITS contract delayed corrective action on multiple information security weaknesses and increased the risk that the Corporation could experience a loss of sensitive information, including personally identifiable information (PII). Second, the omission of SLAs and measures of performance related to information security from the MITS contract reduces the ability of the Corporation to hold its contractor accountable for implementing adequate information security and exposes the Corporation to contract modification requests and requests for additional funding when such SLAs and measures of performance are ultimately developed.

Without a centralized procurement management system, Corporation management may not be fully informed of a specific procurement's status and able to identify and intervene to resolve procurement delays.

Fundamentally, the expiration of the MDCS contract and the six-month extension placed the Corporation's mission at risk. Because the Corporation does not own its IT assets (e.g., network equipment and servers), the MDCS vendor could have ceased providing IT services as of May 31, 2015 or provided such IT services under exorbitantly high rates during the one-month contract extensions. Further, the Corporation's negotiating position for lower rates and/or higher levels of service was significantly weakened, as the incumbent vendor knew the Corporation had limited alternatives.

Without CPARS ratings on file for a vendor, the evaluation panel may not be informed of prior contract "cure" notices or OIG audits or investigations involving the vendor during the source selection process. Finally, regarding limited competition, the Corporation entered into a long-term, seven-year agreement at potentially less favorable market rates and guaranteed levels of service.

Recommendations: Kearney recommends that the Corporation take the following actions:

1. Update the Corporation's standard information security language for contracts to include measures of performance
2. Develop SLAs and measures of performance and incorporate such into the MITS contract
3. Conduct a procurement study to identify opportunities to reduce delays and improve efficiency when awarding contracts. Consider leveraging a Federal shared service provider if in-house resources lack the technical expertise for IT contracts
4. Develop and deliver training for customers of OPS on SOW development and include instructions on completing the Source Selection Determination Memorandum
5. Require CORs to complete CPARS evaluations upon completion of all contracts over $150,000
6. Update the Corporation's procurement procedures and practices to promote increased competition on large procurements. Such practices could include, but are not limited to, hosting an Industry Day, distributing a draft SOW and requesting industry comments, and contacting potential bidders to gauge their willingness to bid, ensuring sufficient competition for an award.

2. Identity and Access Management (IAM)

Finding #2: Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement (*See Appendix E, DHS Question # 1: Continuous Monitoring Management)*

Background: Proactively monitoring IT accounts, including user accounts, privileged-user accounts, and application-level accounts, protects data, equipment, and facilities from unauthorized modification, loss, and disclosure. The OMB and NIST established mandatory security controls that require organizations to create, enable, modify, disable, and remove accounts in accordance with organizational-defined procedures. According to the Corporation's Network System Security Plan (SSP), an automated process executes twice a month to disable accounts that have not been accessed in the prior 30 days. On a monthly basis, the Corporation performs a manual review[18] of all network accounts and deletes accounts that have been disabled for 30 days. Disabling and removing network accounts belonging to departed employees and contractors is an important internal control as the Corporation utilizes the network user ID and password to authenticate individuals to the Corporation's financial system, Momentum, the grants management system, and member management system. Disabling the user's network account removes the user's ability to access Momentum, the grants management system, and the member management system.

In addition to monitoring accounts, NIST requires that Federal agencies periodically review user accounts for separation of duties and the implementation of least privilege.[19] The Corporation determined that it would perform these reviews on a quarterly basis.

Condition: The Corporation's user account access review process was not effective at identifying inactive accounts or accounts belonging to departed employees or contractors due to the manual process involved in granting and removing user account access. Specifically, Kearney noted the following issues:

1. The Corporation's practices allowed user accounts to remain active after 30 days of inactivity on the Corporation's network and sometimes as long as 99 days
2. The Corporation lacked an adequate process to review accounts that were created but never accessed on the network
3. The Corporation did not consistently delete "disabled" accounts that had been disabled for over 30 days as defined in the Corporation's Network SSP
4. The Corporation's off-boarding process was not adequate as departed employees/ contractors' accounts were not removed in a timely manner.

[18] The manual review entails the network System Administrators (SA) inquiring of the individual's supervisor whether a disabled account should be removed or retained.
[19] NIST SP 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, defines least privilege as, "allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

Additionally, the Corporation's process for the quarterly review of Momentum accounts did not require the SA to disable an account if the individual's supervisor failed to confirm the user's access and roles remained valid. For example, on the April 30, 2015 security report used to conduct the quarterly account review for Momentum, 17 of 35 users with inactive accounts were listed under the status "continue to follow up" and had no supervisory confirmation that their continued user access was appropriate. The Momentum SA did not follow up with the supervisors for those 17 Momentum users regarding account status. After inquiry from Kearney in August 2015, those 17 Momentum accounts were subsequently confirmed to be valid with appropriate access roles assigned.

Kearney received a data extract of user accounts from the Corporation's Windows Active Directory (AD) network on June 5, 2015. Using this data extract, Kearney tested for active accounts that had not logged into the network in the prior 30 days (since May 6, 2015), as well as for accounts disabled[20] prior to May 6, 2015. Kearney noted the following exceptions as shown in ***Exhibit 4*** below.

Exhibit 4: Details of Account Management Exceptions

#	System	Observation	Exception
1	Network	One generic account remained active (i.e., enabled) although it had not been logged into since 2012.	A,B
2	Network	One account remained active (i.e., enabled) although the user had not logged into it for 99 days; the account also contained a note "NO LONGER W/CNCS as of 05/15/2015."	A,B
3	Network	Two user accounts remained active (i.e., enabled) although they were unused for 400 days or more; one contained a note stating that the user was "NO LONGER W/CNCS as of 05/03/14."	A,B
4	Network	Two accounts were enabled that had been unused for over 30 days.	A
5	Network	One disabled account, belonging to a user whose departure date was on April 24, 2015 should have been deleted but was not.	B,C
6	Network	Two disabled user accounts, belonging to employees who separated from the Corporation on April 4, 2015 and April 13, 2015, were not timely deleted. Per the Network SSP, these two accounts should have been scheduled for deletion during the April security review and deleted in May 2015.	A,B
7	Network	One account, approved for deletion on May 4, 2015, per Management's Quarterly Review of User Accounts, was not removed during the June monthly account review.	B
8	Momentum	Seventeen of 35 users had a status of "continue to follow up." The Momentum SA did not follow up with the supervisors for those 17 Momentum users regarding account status. After inquiry from Kearney in August 2015, those 17 Momentum accounts were subsequently confirmed to be valid with appropriate access assigned.	D

[20] In a Windows Active Directory network, a user is only able to access the desktop and network resources when the user account has a status of "enabled." To prevent a user from accessing a desktop or other network resource, an administrator sets the user's account to a "disabled" status.

#	System	Observation	Exception
Legend: A: Untimely disablement of inactive account B: Untimely deletion of inactive account C: No documentation of request for authorization revocation D: Account review did not validate user access in a timely manner for 17 users			

Criteria: NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires Federal agencies and organizations to implement account management controls in AC-2 *Account Management*. This control states, in part, that "the organization requires the identification and selection of the types of information system accounts that will support the organizations functions; assigns account managers for information system accounts; specifies authorized users and access authorizations for each account; requires approvals for requests to create information system accounts; and requires organizations to create, enable, modify, disable, and remove information system accounts in accordance with organizational-defined procedures."

In addition, the Corporation's account management standard operating procedures (SOP) provides guidance for managing user, service, and domain administrators (i.e., three-letter accounts) within Windows AD. The SOP states: "Accounts are disabled in the system when a Corporation Exit Form is submitted by the user's manager or when an account has been inactive for 30 days."

Cause: User accounts that belong to departed employees and contractors may remain active after 30 days of inactivity as the Corporation executes the automated disabling script twice a month, rather than nightly. Further, the Corporation's monthly account review is not entirely effective at identifying inactive accounts that should be disabled or disabled accounts that should be deleted due to the manual process involved.

The Corporation stated that prior to June 15, 2015, the on/off-boarding system for employees and contractors was a manual, paper-based process. Under this manual process, when an individual no longer required access, the Office of Human Capital or the contractor program manager was required to contact OIT so that the user ID would be disabled at midnight on the individual's departure date. According to the Corporation's Network SSP, the user account would remain disabled for up to 30 days and then be scheduled for deletion at the next monthly security review. The Corporation's policy is to delete disabled accounts after 30 days. The manual nature of this process allowed many errors when requests for account creation, modification, or termination were not processed in a timely manner.

The Corporation implemented a new on/off-boarding system as of June 15, 2015. The new system involves role-based authentication, where the new hire is required to complete either the Employee On-boarding System (EOS) or the Contractor On-boarding System (COS). Both systems can only be accessed over the Corporation's network and only authorized individuals can create new on-boarding requests. By contrast, no official role is required to initiate an off-boarding request. In order for an employee/contractor to complete the off-boarding process, the departing or transferring employee/contractor must acknowledge a change in status. The procedure is a precaution used to verify appropriateness of change requests. When the off-boarding process is initiated, each Corporation office gets a concurrent notification confirming the access revocation. The required steps to complete the off-boarding process can be completed concurrently, and the new system is designed to allow visibility into the workflow of the process. The Corporation stated that the new system would strengthen the account management review process and improve the employee's/contractor's off-boarding process.[21]

Effect: Without adequate access controls, unauthorized individuals, including former Corporation employees or contractors, may access sensitive information including PII. As the Corporation collects significant quantities of PII in the administration of grants and educational awards, there is a risk of data loss and potentially unauthorized changes to grant or educational award information.

Regarding Momentum user access, without periodic account review for appropriateness, individuals may accumulate excess access privileges or have access rights that are incompatible[22] with their current job functions.

Recommendations: Kearney recommends that the Corporation:

7. Execute the automated script to disable inactive accounts on a nightly basis, rather than current practice of twice a month, to enforce the Corporation's policy to disable accounts that have not been accessed in the prior 30 days
8. Automate the current manual account review process to delete accounts set as "disabled" after 30 days. For disabled user accounts that should not be deleted due to circumstances such as medical leave, the user account should be moved into a special AD Organizational Unit that is not subject to automatic deletion
9. Require SAs to disable accounts timely after completion of the quarterly account review process unless they receive confirmation that user access remains appropriate.

[21] Kearney observed a walkthrough of the new system prior to its deployment but did not test the new on/off-boarding system.
[22] An example of incompatible functions within Momentum would be for an individual user to hold both the "Cash Receipts Entry" and the "Cash Receipts Approval" job roles; the Corporation desires to separate the activities of recording cash receipts from the review and approval function.

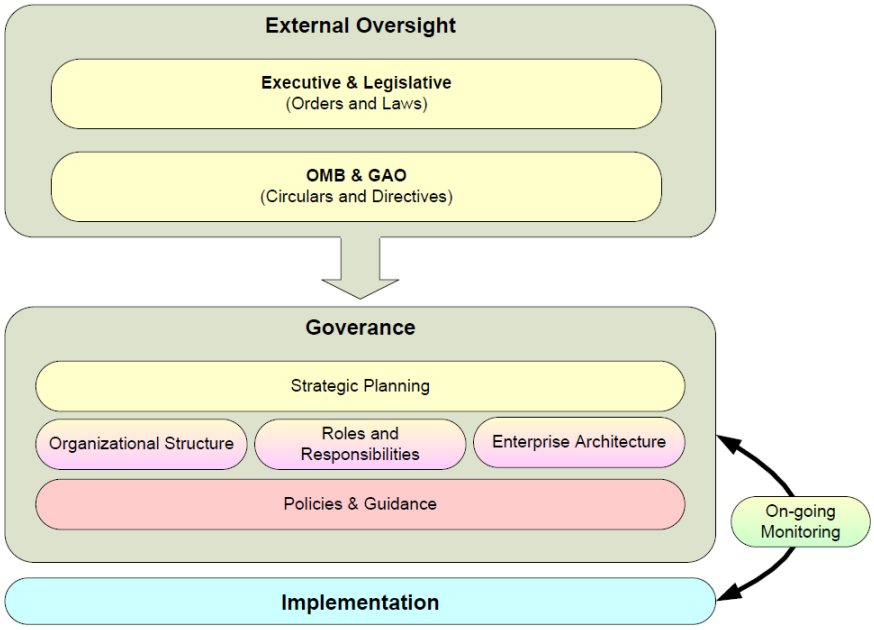
3. Continuous Monitoring

Finding #3: Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan (*See Appendix E, DHS Question # 1: Continuous Monitoring Management)*

Background: An IT strategic plan should be developed in light of the business needs of an organization and to ensure that the organization's IT capabilities has the ability and direction to meet those business needs. The mission of the Corporation is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. Thus, the Corporation's IT strategic plan highlights how IT resources will be utilized to provide solutions that support its missions, initiatives, and priorities. Likewise, the Enterprise Architecture Plan (EAP) provides a roadmap for implementation that explicitly defines the types of data, applications, hardware, and software that are appropriate for and support the overall organization's network/enterprise.

IT strategic plans and EAPs are essential to ensure that the Corporation makes informed decisions about its needs and intended approach **before** making a significant financial commitment. The IT strategic plan and EAP should be used collaboratively to support the Corporation's core business processes and ensure secure and reliable delivery of IT solutions to the Corporation. Adequate planning ensures the Corporation adopts appropriate IT solutions for OIT's IT modernization efforts to ensure business prioritization and efficient use of limited resources while meeting Federal security and privacy standards. ***Exhibit 5*** depicts the relationship between IT strategic planning, organizational design and development, and integration with the enterprise architecture.

Exhibit 5: Information Security Governance Components



Source: NIST SP 800-100 Information Security Handbook: A Guide for Managers.

Condition: Kearney noted that the Corporation's current IT strategic plan was last updated in FY 2013 and does not reflect current IT modernization efforts. Specifically, the IT strategic plan does not describe the Corporation's long-term goals and strategies for leveraging IT to satisfy business needs. Additionally, the IT strategic plan does not describe a strategy to protect sensitive information and PII in a cloud environment while satisfying Federal information security requirements. Furthermore, the Corporation has not defined how its information security investments and security strategy fits into the IT strategic plan. Finally, the Corporation has not created an EAP.

The CIO informed Kearney that the Corporation intends to implement cloud-based computing[23] to deliver increased business value and reduced operational costs. Before embracing the cloud-computing model, the Corporation should ensure that its chosen approach provides sufficient data protection for securing PII. Further, the Corporation should confirm its chosen cloud service provider provides data portability, meaning the Corporation could move its data to another cloud provider without technology lock-in or significant costs. The value of developing an IT strategic plan and EAP is the rigor and preparation brought to the Corporation before significant financial investments are made.

Criteria: The Paperwork Reduction Act of 1995 (PRA) requires all Federal agencies to implement an IT strategic plan. The legislation states: "With respect to general information resources management, each agency shall -- develop and maintain a strategic information resources management plan that shall describe how information resources management activities help accomplish agency missions."

Similarly, the Clinger-Cohen Act of 1996 requires agencies to leverage a disciplined capital planning and investment control (CPIC) process to acquire, use, maintain, and dispose of IT resources. The Federal Information Security Management Act of 2002 (FISMA-2002) states: "In general, the head of each agency shall -- (C) ensuring that information security management processes are integrated with agency strategic and operational planning processes."

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, states:

> "Agencies should identify applicable requirements based on relevant legislation, regulations, federal directives, and agency-level directives. Agencies should also ensure that information security governance structures are implemented in a manner that best supports their unique missions and operations. Agencies should integrate their information security governance activities with the overall agency structure and activities by ensuring appropriate participation of agency officials in overseeing implementation of

[23] NIST SP 800-145, *The NIST Definition of Cloud Computing*, defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud-computing model is composed of the following five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

information security controls throughout the agency. The key activities that facilitate such integration are ***strategic planning***, organizational design and development, establishment of roles and responsibilities, integration with the ***enterprise architecture***, and documentation of security objectives in policies and guidance."

Regarding the lack of a documented EAP, NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control PM-7 *Enterprise Architecture* states: "The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes."

Cause: In FY 2014, the CIO and Chief Information Security Officer (CISO) left the Corporation. The prior CIO did not believe it was necessary or required to implement and maintain an IT strategic plan or an EAP. Thus, the IT strategic plan was not updated and an EAP was not developed during the tenure of the prior CIO when the Corporation started its FY 2014-2016 IT modernization efforts. Subsequently, the Corporation appointed a new CIO in March 2015, as well as a new CISO and Security Analyst in June 2015. The lack of a permanent CIO for six months and a CISO for nine months, as well as other IT vacancies, prevented the development of long-range plans, as OIT resources were focused on day-to-day operational challenges. The current CIO indicated that the Corporation plans to update its IT strategic plan in the second quarter of FY 2016 but did not provide a specific timeframe for the completion of an EAP.

Effect: Failure to develop and implement an IT strategic plan can result in the inefficient use of scarce resources and wasteful IT investments due to lack of an overall coordinated IT strategy. As the Corporation has made a conscious decision to outsource many aspects of IT operations, the lack of a written IT strategic plan and supporting EAP allows its IT vendors to select technologies and solutions that benefit the Corporation's short-term needs but may not address its long-term strategies or provide the Corporation flexibility to migrate its data to another cloud provider. Further, without appropriate analyses and planning, the Corporation's IT investments may not provide sufficient protections (e.g., encryption of data at rest, audit logging of PII extracts, etc.) over sensitive PII required of Federal organizations. Attempting to retrofit security and privacy requirements into a deployed cloud-based solution may not be feasible or cost-effective.

Recommendations: Kearney recommends that the Corporation:

10. Immediately update its IT strategic plan by:
    a. Including current IT modernization efforts and future IT investments
    b. Updating performance metrics to measure success and determine if milestones are being reached
    c. Defining roles and responsibilities of identified human resources
    d. Periodically updating the strategic plan to reflect major changes in IT strategy

11. Immediately develop an EAP by:
    a. Highlighting the target solutions, technologies, and security requirements
    b. Periodically updating the EAP to mirror any changes and remain in sync with the IT strategic plan.

4. Risk Management

Finding #4: Inaccurate Inventory of Physical Information Technology Asset (*See Appendix E, DHS Question # 5: Risk Management)*

Background: Maintaining a complete, accurate, and up-to-date inventory of physical IT assets is essential to implementing an effective Security and Risk Management Program. Most organizational IT infrastructures have various types of physical IT assets at multiple locations. Effectively tracking IT assets across multiple locations and IT platforms helps prevent loss and theft. Maintaining a current, accurate inventory of physical IT assets also facilitates reconciling IT assets with financial records, such as equipment leases and software licenses. The CIO informed Kearney that the Corporation has three major inventory tracking systems.[24] The CIO also mentioned that the Corporation is planning to consolidate the three major inventory tracking systems into one master inventory database. Kearney's audit procedures focused on validating the accuracy and completeness of the current physical IT assets to ensure all physical IT assets existed and were assigned to the correct individuals to promote accountability.

Condition: On July 30, 2015, Kearney visited the Philadelphia Field Financial Management Center (FFMC) and the Pennsylvania State Office. The following day, Kearney visited the Baltimore National Civilian Community Corps (NCCC) and the Maryland State Office to evaluate the accuracy of the sites' IT inventory. Kearney noted that none of the sites had an accurate inventory of physical IT assets maintained onsite and that some physical IT assets that were onsite were not listed on the inventory spreadsheet. Specifically, Kearney noted the following:

Maryland State Office

- Despite multiple inquiries from Kearney, neither Corporation Headquarters nor the Maryland State Office staff were able to provide an inventory list of physical IT assets.

NCCC Baltimore Campus

- The "Item Number/Serial Number" was not recorded on the IT inventory list for six IT assets (Asset Numbers #52577, #92253, #93345, #93858, #30745, and #52348)
- An external 2 Terabyte (TB) Passport External Hard Drive (Asset #52578) was not recorded on the inventory list
- Kearney identified a Support Services Specialist (campus staff), who also serves as the Computer Hardware Property Custodian and is responsible for maintaining an Excel spreadsheet of campus inventory items. The Computer Hardware Property Custodian updates the IT inventory when new items are received or when items are shipped out to

[24] Three inventories tracking systems are Corporation Headquarters IT assets (e.g., laptops, monitors, printers, servers, etc.); personal property inventory (e.g., desks, chairs, etc.); and NCCC inventory (e.g., shovels, tools, etc.).

Headquarters for service or another NCCC site for a temporary loan. However, Kearney noted nine instances on the campus inventory where the IT asset was assigned to the incorrect person or location (Asset Numbers #92330, #92983, #92984, #93084, #93186, #93325, #93551, #93563, and #93589).

FFMC

- Three IT assets were not recorded on the IT inventory list (Asset Numbers #90095, #91086, and #70393).

In the FY 2014 FISMA evaluation, Kearney noted similar IT inventory issues related to inaccurate asset tracking during the Volunteers in Service to America (VISTA) Member Support Unit (VMSU) site visit.

Criteria: Corporation policy, *OIT Property Management*, Policy Number 377 (Rev. 4), states, in part:

"All Corporation field offices will follow the guidelines listed below:
Each State Office Director, NCCC Campus Director, and FFMC Director must:

i. Designate in writing or assume the responsibility of Computer Hardware Property Custodian for that location. The name of the Computer Property Custodian must be e-mailed to the PM, Infrastructure Services, and the Customer Service Specialist of the Office of Information Technology (OIT)
ii. Conduct an annual inventory of computer hardware at that location, consistent with specific instructions provided by OIT
iii. Ensure that the computer hardware that is no longer needed is sent back to OIT. When computer hardware is no longer needed, please ship it back in a safe box with the computer hardware wrapped in bubble wrap and have it sent back through UPS as soon as possible. Please do not use any shredded material
iv. Ensure computer property is adequately controlled, accounted for, and used as effectively and economically as possible
v. Ensure that employees who leave Corporation employment have returned their assigned property
vi. Provide current inventory information to OIT upon request."

NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires Federal agencies and organizations to implement component inventory controls in CM-8 *Information System Component Inventory*. This control states, in part, that "the organization requires the establishment of an inventory of system components that accurately reflects the current system; includes all components within the authorization boundary of the information system; and reviews and updates the information system component inventory."

Cause: The Corporation did not perform adequate reviews and consolidation of inventory lists at remote offices. The Corporation and the remote locations utilized multiple Excel spreadsheets to track physical IT assets, rather than a single, centralized database, which made it difficult to manage and reconcile among multiple sources. Further, the Corporation did not follow its documented process in the *OIT Property Management* policy to effectively manage the physical IT assets. Also, during the FFMC site visit, the FFMC Director informed Kearney that the Corporation provided FFMC employees with new laptops at the same time as the FFMC performed its annual IT assets inventory. The laptop refresh at the FFMC contributed to the noted errors on the IT inventory list, as some individuals had multiple or the wrong IT assets assigned to them. Furthermore, the Corporation's staff at the Philadelphia FFMC and Baltimore NCCC were allowed to take over computer monitors from departing employees without officially reporting the change of IT asset assignment to the OIT at Headquarters. Collectively, these factors contributed to the additional errors in the master inventory list maintained by the OIT.

Effect: Without maintaining a complete, accurate, and up-to-date IT inventory, the Corporation cannot effectively prevent waste, fraud, and abuse. Periodic, physical inventories of IT assets ensure all assets are appropriately accounted for and business records are accurate. Based on inaccurate physical inventories of laptops and desktops, the Corporation could pay unnecessary software licensing fees for laptops and desktops that are not used. Finally, not maintaining an updated inventory could result in loss or theft of equipment and potentially sensitive information. The loss of sensitive information, such as PII or Protected Health Information (PHI), could cause significant financial loss to the Corporation.

Recommendations: Kearney recommends that the Corporation:

12. Continue with the current plan to implement a single, centralized database to manage agency-wide physical inventory
13. Update and communicate procedures for updating the inventory list when a laptop, monitor, or other physical IT asset is assigned to or retrieved from a user
14. Perform biannual physical IT inventory audits at Headquarters and field offices to ensure the IT inventory list and assignments of physical IT assets are accurate
15. Perform periodic validation of the IT asset inventory in comparison with active network devices to identify potentially missing laptops and desktops.

APPENDIX B: STATUS OF PRIOR YEAR FINDINGS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our" in this report) followed up on the status of the Notice of Findings and Recommendations (NFR) reported in the Federal Information Security Management Act of 2002 (FISMA) Independent Evaluation for Fiscal Year (FY) 2014, Office of Inspector General (OIG) Report 15-03[25]. Among our reported findings from FY 2014, we concluded that the Corporation for National and Community Service (the Corporation) closed three out of sixteen findings from the FY 2014 FISMA evaluation and implemented nine of 67 recommendations. The three closed findings were "Lack of Controls to Prevent Use of Unauthorized Devices," "Lack of Segregation of Duties," and "Inadequate Incident Response Reporting." See the summary below for the status of FY 2014 NFRs as of September 2015.

Resolution Status of FY 2014 Notice of Findings and Recommendations

FY 2014 FISMA Reporting Area Summary of NFRs	FY 2013 Repeat Finding	FY 2014 Severity	FY 2015 Status	FY 2015 Severity
Continuous Monitoring Management				
1. Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy	X	Significant Deficiency	In Progress	Significant Deficiency
2. Multiple Weaknesses with Vulnerability Scanning and Remediation		Significant Deficiency	In Progress	Significant Deficiency
3. Organizational Conflict of Interest		Significant Deficiency	In Progress	Significant Deficiency
4. Use of an Obsolete and Unsupported Network Monitoring Tool		Significant Deficiency	In Progress	Significant Deficiency
Configuration Management				
5. Lack of Controls to Prevent Use of Unauthorized Devices		Control Deficiency	Done	N/A
6. Risks to the Confidentiality and Availability of Voice Communications		Control Deficiency	In Progress	Control Deficiency
Identity and Access Management				
7. Lack of Segregation of Duties (SoD)		Control Deficiency	Done	N/A
Incident Response and Reporting				
8. Inadequate Incident Response Reporting		Control Deficiency	Done	N/A

[25] For the full text of the FY 2014 FISMA report, visit http://www.cncsoig.gov/sites/default/files/15-03_0.pdf.

FY 2014 FISMA Reporting Area Summary of NFRs	FY 2013 Repeat Finding	FY 2014 Severity	FY 2015 Status	FY 2015 Severity
Risk Management				
9. Inadequate Enterprise-Wide Risk Management Policies and Practices	X	Control Deficiency	In Progress	Control Deficiency
10. Weaknesses with the Corporation's Security Planning and Assessment Process	X	Significant Deficiency	In Progress	Significant Deficiency
Security Training				
11. Lack of Formal, Role-Based Training	X	Control Deficiency	In Progress	Control Deficiency
Plans of Action and Milestones (POA&M)				
12. Improvements Needed to POA&M Reporting	X	Significant Deficiency	In Progress	Control Deficiency
Remote Access Management				
13. Inadequate Controls over Remote Access		Control Deficiency	In Progress	Control Deficiency
Contingency Planning				
14. Inadequate Disaster Recovery Plan (DRP) Documentation and Planning		Control Deficiency	In Progress	Control Deficiency
15. Lack of Adequate Testing of Continuity of Operations Plan (COOP)		Control Deficiency	In Progress	Control Deficiency
Privacy				
16. Inadequate Controls over Privacy Data		Significant Deficiency	In Progress	Control Deficiency

Fiscal Year 2014 Finding #1: Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring Strategy[26]

The Corporation has not formally documented and implemented an organization-wide ISCM Program and strategy, as mandated by the Office of Management and Budget (OMB) guidance; and as required by several National Institute of Standards and Technology (NIST) Special Publications (SP), including NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; and NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

FY 2015 Update:

In the FY 2013 and 2014 FISMA evaluations, Kearney reported similar weaknesses associated with developing and implementing the Corporation's ISCM process. Resource constraints precluded the Corporation from developing and implementing an ISCM Program prior to filling various key IT position vacancies. The Corporation has taken a number of important steps to address the prior year's weaknesses. These steps include hiring a Chief Information Security Officer (CISO) and Security Analyst in June 2015 and hiring a contractor in May 2015 to support the development of the Corporation's Information Security Program. Additionally, the Corporation established a Memorandum of Agreement (MOA) in November 2014 with the Department of Homeland Security (DHS), Office of Cybersecurity and Communications (CS&C) to participate in DHS's Continuous Diagnostics and Mitigation (CDM)[27] Program.

Despite these preliminary steps, progress towards resolving fundamental weaknesses within the Corporation's ISCM[28] Program has been limited and serious vulnerabilities

[26] For full text of this prior year finding, please refer to page 18 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.
[27] DHS defines the CDM Program as an approach to fortifying the cybersecurity of Government networks and systems. CDM provides Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.
[28] As stated in NIST SP 800-137, the ISCM strategy should be: 1) grounded in a clear understanding of organizational risk tolerance and help officials set priorities and manage risk consistently throughout the organization; 2) include metrics that provide meaningful indications of security status at all organizational tiers; 3) ensure continued effectiveness of all security controls; 4) verify compliance with information security requirements derived from organization missions/business functions, Federal legislation, directives, regulations, policies, and standards/guidelines; 5) be informed by all organizational information technology (IT) assets and help maintain visibility into the security of the assets; 6) ensure knowledge and control of changes to organizational systems and environments of operation; and 7) maintain awareness of threats and vulnerabilities.

remain. ISCM requires that the Corporation develop and maintain an enterprise-wide Continuous Monitoring Program that assesses the security state of information systems, consistent with FISMA requirements, OMB policy, and applicable NIST guidelines, and provides an adequate basis for organizational risk management decisions. As of the completion of fieldwork in August 2015, the Corporation had not finalized an ISCM strategy. The draft ISCM strategy document was not complete and contained multiple highlights and reviewer comments, demonstrating that additional work is needed.

Critically, the ISCM draft did not identify performance metrics that were meaningful and reportable for all business processes supporting the Corporation's mission. Examples of frequently used information security metrics advocated by NIST include number of opened and closed POA&Ms during a period, overdue POA&Ms, security patches deployed within the Corporation's established timeframes, and an aging analysis (e.g., under 30 days, 30-60 days, over 60 days, etc.) of critical and high-risk security weaknesses from the Corporation's vulnerability scanner. Without such metrics, monitoring is likely to be haphazard, subjective, and not amenable to oversight by agency leaders.

The Corporation made less progress than originally planned addressing the ISCM weaknesses as it was without a CISO and Security Analyst for nine months of FY 2015. Additionally, the eight-month delay awarding the Managed Information Technology Services (MITS) contract[29] prevented the Corporation and its vendor from replacing critical technology for vulnerability scanning and network monitoring.

Under the maturity model for ISCM Programs developed by the Council of the Inspectors General for Integrity and Efficiency[30] (CIGIE), the Corporation received the lowest score—one out of five—signifying that, as of August 30, 2015, its ISCM Program was not formalized and that its ISCM processes were not consistently performed, resulting in an ad hoc program. The attributes of a Level 1: ad hoc versus a more mature, Level 3: consistently implemented ISCM Program are available on DHS's website and contained within the annual FISMA reporting instructions to Inspector Generals. Kearney assessed the Corporation's ISCM Program as ad hoc in each of the three required evaluation areas (i.e., People, Processes, and Technology).

FY 2014 Recommendations	FY 2015 Status
16. Document and fully implement an organization-wide, comprehensive ISCM strategy that incorporates Tier 1 and Tier 2 levels.	In Progress
17. Improve oversight over IT service providers.	In Progress

[29] See related FY 2015 new FISMA finding: *Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses.*
[30] CIGIE is an independent entity established within the Executive branch to address integrity, economy, and effectiveness issues that transcend individual Government agencies and aid in the establishment of a professional, well-trained, and highly skilled workforce in the Offices of Inspectors General.

18. Formalize ISCM processes to include the following:	
a. Establishment of metrics to be monitored.	In Progress
b. Establishment of frequencies for monitoring/assessments.	In Progress
c. Approach for ongoing security control assessments and status monitoring to determine the effectiveness of deployed security controls.	In Progress
d. Correlation and analysis of security-related information generated by assessments and monitoring.	In Progress
e. Response actions to address the results of the analysis.	In Progress
f. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.	In Progress

Fiscal Year 2014 Finding #2: Multiple Weaknesses with Vulnerability Scanning and Remediation[31]

Kearney identified five deficiencies related to vulnerability scanning and the remediation process at the Corporation. Specifically, the Corporation did not:

1. Scan desktops and laptops on a monthly basis for missing security patches and/or configuration errors
2. Review monthly scan results of servers for 10 months, and as a result, allowed 39 high-risk vulnerabilities to continue
3. Configure the vulnerability scanner to identify missing security patches belonging to frequently exploited applications, such as Internet Explorer, Microsoft Office, Adobe Reader, Adobe Flash, and Java
4. Perform a scan for configuration errors and deviations from the United States Government Configuration Baseline (USGCB)[32]
5. Include performance metrics for the timely remediation of identified vulnerabilities in the Managed Data Center Services (MDCS) contract or other IT contracts.

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control RA-5: "Vulnerability Scanning" requires Federal agencies and organizations to scan for vulnerabilities in the information system and hosted application, analyze vulnerability scan reports and results from security control assessments, and remediate legitimate vulnerabilities.

FY 2015 Update:

The Corporation has taken some steps, but with limited progress, to resolve the prior year weaknesses, including awarding the MITS contract (formerly MDCS contract) on July 30, 2015, which requires contractor support for the full scope of IT infrastructure services. The new MITS contract requires vendors to comply with the Corporation's Information Assurance Policy; however, it does not mandate that the vendor replace the existing vulnerability scanner or test and deploy security patches based on risk within prescribed timeframes.[33]

Weaknesses remain with vulnerability scanning and patch remediation. Prior to March 2015, the Corporation's vulnerability scanning process, administered by its MDCS provider, included only servers and routers. The Corporation also ceased installing Microsoft security patches from

[31] For full text of this prior year finding, please refer to page 22 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.
[32] USGCB is a secure configuration standard for Windows XP, Vista, and Windows 7 desktop that specifies over 550 secure settings that NIST maintains and updates in response to new security vulnerabilities. The large number of security settings means that manual review is impractical without the use of an automated tool that supports the SCAP protocol.
[33] See related FY 2015 new FISMA finding: on *Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses.*

August 2014 through December 2014 when the Corporation deployed Microsoft Office 365.[34] Additionally, the Corporation did not provide evidence of periodic scanning on its desktops and laptops for USGCB compliance. Prior to February 2015, the Corporation used a vulnerability scanning tool that was not compliant with NIST standards and did not support the Security Content Automation Protocol (SCAP)[35].

As a result, the Corporation was unable to demonstrate that its desktops and laptops were securely configured to the USGCB standard version 1.2. Although the Corporation upgraded the vulnerability scanning tool in February 2015 to a version that supports SCAP and could evaluate compliance with USGCB, the Corporation did not provide evidence that USGCB compliance scans were performed with the upgraded vulnerability scanning tool as of August 31, 2015.

To evaluate the Corporation's actions to identify and correct prior year weaknesses, we performed vulnerability scans on 177 Windows servers and 273 workstations. We noted the following results as of July 28, 2015:

- Windows Servers contained 1,973 critical and 3,927 high-risk vulnerabilities[36]
- Workstations contained 932 high-risk vulnerabilities.

The July 28, 2015 vulnerability scanning results did not include two of the Corporation's major applications (i.e., eGrants and Electronic-System for Programs, Agreements, and National Service Participants [eSPAN]), as we received bad network credentials and a secondary firewall did not allow traffic from our vulnerability scanner to the database servers that support eGrants and eSPAN. Through troubleshooting this technical issue, we discovered that the Corporation has never performed an authenticated scan of the eGrants and eSPAN database servers due to incorrect firewall rules. Subsequently, the Corporation reconfigured the eGrants and eSPAN firewall to allow network traffic for our vulnerability scan of eGrants and eSPAN.

On September 9, 2015, Kearney performed a second vulnerability scan on three eGrants servers and two eSPAN servers, noting the following:

- eGrants servers contained 84 high-risk vulnerabilities
- eSPAN servers contained 58 high-risk vulnerabilities.

[34] Microsoft Office 365 is a group of software plus services subscriptions that provides productivity software, such as e-mail and SharePoint, to its subscribers.
[35] SCAP is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.
[36] Vulnerabilities are reported in Tenable Nessus Pro with a severity of critical, high, medium, or low to allow appropriate prioritization of remediation efforts. Vulnerability severity is determined using the Common Vulnerability Scoring System (CVSS). CVSS is an open industry standard for assessing the severity of computer system security vulnerabilities; it attempts to establish a measure of how much concern a vulnerability warrants, compared to other vulnerabilities. The scores range from 0 to 10.

As of September 9, 2015, the Corporation had not established performance metrics to measure the timeliness of patch remediation or implemented a new vulnerability scanning tool.

A key goal of configuration management is to make IT assets harder to exploit through better configuration. The configuration management capability needs to: be complete (e.g., cover enough of the software base to significantly increase the effort required for a successful attack); operate in near-real-time (less than 72 hours) (e.g., able to find and fix configuration deviations faster than they can be exploited); be accurate (e.g., have a low enough rate of false positives to avoid unnecessary effort and have a low enough rate of false negatives to avoid unknown weaknesses); and be implemented in a manner that promotes system accuracy and integrity over time.

Without performance metrics and supporting tools to measure timeliness and completeness of security patch deployments and secure configurations of its desktops and servers, the Corporation may not be aware of its security vulnerabilities and able to take prompt, corrective action.

FY 2014 Recommendations	FY 2015 Status
19. Establish performance metrics for the timely remediation of high-, moderate-, and low-risk vulnerabilities. Consider sharing the results with the system owner and Information System Security Officer (ISSO) to increase visibility and awareness of unresolved and outstanding weaknesses.	In Progress
20. Include performance metrics for vulnerability management in future MDCS contracts.	In Progress
21. Update the Multiprotocol Label Switching (MPLS) network's configuration and Windows desktop firewalls to allow the Corporation's vulnerability scanning tool(s) to successfully communicate.	Closed
22. Test workstation performance during intrusive scans to determine the feasibility of obtaining comprehensive vulnerability scan results.	Closed
23. Periodically perform scans of desktops and laptops using the current USGCB template from NIST to ensure ongoing compliance.	In Progress
24. Upgrade or replace the Corporation's vulnerability scanning tool to overcome existing limitations and inaccurate scan results.	In Progress
25. Implement a monthly process to review vulnerability scan configurations to include new vulnerability checks prior to scan execution.	In Progress
26. Ensure that an appropriately configured vulnerability scan is conducted monthly against all information system components, including servers, routers, desktops, network printers, scanners, and copiers.	In Progress
27. Strengthen oversight of the Corporation's IT contractors to ensure that vulnerability scan results are complete and reviewed and confirm that identified weaknesses are remediated in a timely manner based on risk.	In Progress

Fiscal Year 2014 Finding #3: Organizational Conflict of Interest[37]

NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, control CA-2(1) requires that security assessors be independent and impartial when performing security assessments for FIPS 199-rated "moderate" and "high" impact information systems. The Corporation permitted its MDCS contractor to perform the Security Assessment and Authorization (SA&A) of the Corporation's General Support System (GSS) and eSPAN information systems rather than requiring that the MDCS contractor hire an independent party. The security assessors, who had primary responsibility for monitoring the Corporation's network, worked for the MDCS contractor and reported to the overall Project Manager. The security assessors were effectively reviewing their own work and that of their colleagues, and their employment status, assigned job responsibilities, and organizational reporting relationships precluded an impartial and objective evaluation of security controls. The resulting System Security Plan (SSP), Security Assessment Report (SAR), and POA&Ms contained multiple factual errors, inconsistencies, and omissions that called into question the objectivity and rigor of the security assessment for the network GSS and eSPAN, as well as the quality of the Corporation's oversight of the SA&A.

FY 2015 Update:

In October 2014, the Corporation acknowledged that an organizational conflict of interest existed and indicated its intent to correct the issue through the re-compete of the MDCS contract. The Corporation has taken some steps, but with limited progress, to resolve the prior year weaknesses by hiring an independent Information Assurance Program Support (IAPS) contractor in May 2015 to perform a review and validation of security assessments performed by the Corporation's IT vendors. However, the IAPS contractor had not completed any independent security assessments as of August 2015 when fieldwork was completed. During the period of October 1, 2014, to July 31, 2015, the MDCS contractor continued prior practices of performing security control self-assessments. In August 2015, the Corporation awarded a new MITS contract to replace the MDCS contract. As reported in the FY 2015 new finding, *Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses*, the new MITS contract did not include contract requirements that the SA&A be performed by an independent assessment team.

FY 2014 Recommendations:	FY 2015 Status
28. Ensure that all IT contracts contain clear and enforceable provisions for an independent, in both fact and appearance, SA&A process or that a separate contract is established to conduct the SA&A process by an independent third party.	In Progress
29. Ensure that the Contracting Officer's Representative (COR) enforces all provisions contained within contracts or a formal contract modification is to explicitly account for changes issued through the Contracting Officer (CO).	In Progress

[37] For full text of this prior year finding, please refer to page 27 of the published OIG Report Number 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

30. Strengthen oversight of the Organization's' IT contractors to ensure implementation of the SA&A process complies with Federal standards.	In Progress

Fiscal Year 2014 Finding #4: Use of an Obsolete and Unsupported Network Monitoring Tool[38]

The Corporation's primary tool for network monitoring and audit log analysis was obsolete and unsupported by Cisco. Cisco issued an announcement in May 2008 that it would end maintenance support (i.e., patches) in November 2011 and final hardware support in November 2013. However, the Corporation and its MDCS contractor did not replace the tool. Further, the monitoring tool did not retain audit events for a long enough period (i.e., limited to approximately 60 days) to allow useful aggregation to identify trends and perform targeted analysis. In addition, the MDCS contractor had not developed standard operating procedures (SOP) requiring periodic review and maintenance of the audit alert rules. The Corporation also had not established performance metrics to increase accountability for network and audit log monitoring; improve effectiveness of information security; demonstrate compliance with Corporation policy, laws, and regulations; and identify areas for improvement.

The Corporation's contract with the MDCS contractor included a hardware refresh requirement. However, the Corporation did not exercise its contractual rights and request that the MDCS contractor replace the Monitoring Analysis and Response System (MARS)[39] tool prior to the product's End-of-Life (EOL).

FY 2015 Update:

The Corporation has taken some steps to resolve the prior year weaknesses, though vulnerabilities persist at the end of FY 2015. With the award of the MITS contract in August 2015, the Corporation has entered into a contract for a technology refresh and indicated its plans to replace its network monitoring tool, Cisco MARS, with a Security Information Event Management (SIEM) solution called Splunk.[40] To provide additional continuous monitoring capabilities, the Corporation indicated its intent to implement Tenable Security Center[41] and SolarWinds to supplement current network monitoring capabilities.

However, as of September 2015, the Corporation continued to use the obsolete Cisco MARS[42] tool as the primary means for network monitoring and audit log analysis. Further, the new MITS contract does not contain a requirement to utilize hardware and software with vendor

[38] For full text of this prior year finding, please refer to page 30 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.
[39] Cisco MARS is an appliance for logging, analysis, and retention. The tool is designed to detect changes to network devices and servers through log analysis. Cisco announced EOL on May 5, 2008; the Corporation and the GSS contractor did not identify and implement a replacement tool before support ended on November 30, 2011.
[40] Splunk is an appliance that captures, indexes, and correlates real-time data in a searchable repository from which it can generate graphs, reports, alerts, dashboards, and visualizations.
[41] The Corporation will require the Network GSS contractor to use Nessus vulnerability scanner as part of the MITS contract.
[42] Cisco announced EOL for the MARS tool in May 2008, ceased maintenance support (i.e., patches) on November 30, 2011, and stopped all technical support on November 30, 2013. MARS needs to be replaced as it is the Corporation's primary continuous monitoring tool.

support; rather, the contract only requires the provider to "support technology refreshes of all systems and software up to and including the current Operations, Engineering and Maintenance (OEM) production release/version." Thus, if similar circumstances occur in future where a hardware or software vendor ceases to support an installed product, the Corporation is unable to compel the MITS contractor to select a replacement tool that provides equivalent or superior functionality without a change order and request for additional funding.	
FY 2014 Recommendations	**FY 2015 Status**
31. Identify and implement a replacement tool for network monitoring and audit log analysis to regain vendor software and hardware support.	In Progress
32. Strengthen oversight of the Corporation's network monitoring and audit log process to ensure that monitoring tools and associated configurations are properly maintained to detect new threats.	In Progress
33. Ensure IT contracts include clauses requiring contractors to only utilize tools that have both software and hardware support (as applicable).	In Progress
34. Ensure network monitoring and audit log software can maintain audit events online for a sufficient time period that allows for trend analysis and subsequent review and, if necessary, security incident investigation.	In Progress
35. Ensure network monitoring and audit log software can archive audit logs while still observing the National Archives and Records Administration's (NARA) 12-month retention requirement for security audit logs.	In Progress
36. Develop and implement performance metrics to increase accountability for network monitoring and audit log review; improve effectiveness of information security; demonstrate compliance with Corporation policy, laws, and regulations; and identify areas for improvement.	In Progress

Fiscal Year 2014 Finding #5: Lack of Controls to Prevent Use of Unauthorized Devices[43]

The Corporation did not implement IT security policies and supporting technical controls to prevent the use of non-Corporation-issued portable data storage devices (e.g., Universal Serial Bus [USB] thumb drives, external USB hard drives, smart phones, and tablets). In addition, the Corporation did not require employees and contractors to use only agency-issued storage media or to use only federally approved cryptographic algorithms to store personally identifiable information (PII).

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, requires Federal agencies to encrypt all data on mobile computers/devices that carry agency data, unless the data is determined to be non-sensitive, in writing, by the Deputy Secretary or an individual he/she may designate in writing.

FY 2015 Update:

The Corporation has taken steps to resolve the prior year weaknesses. The Corporation implemented a policy requiring the use of Removable Media Encryption (BitLocker USB Encryption) on May 14, 2015. The Microsoft BitLocker service is used to protect data on removable media such as flash drives and portable hard drives. Upon insertion of an unencrypted USB drive into a Corporation desktop or laptop, the BitLocker USB Encryption solution forces encryption of the compatible removable media and prevents writing to an unencrypted device. In addition, on September 30, 2015, the Corporation implemented a new Rules of Behavior, which offers additional guidance regarding user behavior and personal devices.

FY 2014 Recommendations	FY 2015 Status
37. Clarify and enforce the policy on the use of personal devices and USB storage devices for Corporation business and specify any required security controls or use restrictions. Clarification should include differentiation between personal bring your own devices (BYOD) and Corporation-issued devices.	Closed
38. Monitor the use of USB storage devices connected to the Corporation's computers and evaluate the risks presented by their use.	Closed
39. Complete the implementation of automatic encryption, included in the roll-out of Microsoft Office 365, for portable data storage devices for user groups who regularly handle sensitive information (e.g., Procurement, Human Resources, IT).	Closed

[43] For full text of this prior year finding, please refer to page 33 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Fiscal Year 2014 Finding #6: Risks to the Confidentiality of Voice Communications[44]

The Corporation does not logically isolate its voice network traffic from its data network. Specifically, Corporation desktops were able to ping (query) Cisco Voice over Internet Protocol (VoIP) phones at remote offices. In addition, users were able to access the Cisco VoIP phones using their desktops' web browsers over hypertext transfer protocol (HTTP). Permitting network traffic between the voice and data networks exposes the voice network to multiple attack vectors and security weaknesses. This could be exploited by malicious individuals to compromise VoIP components, which generally were not designed with security in mind, and could allow an attacker to intercept and record phone calls. NIST specifically recommends against connecting voice and data networks, stating, "separate voice and data on logically different networks, if feasible," in SP 800-58 *Security Considerations for Voice Over IP Systems.*

FY 2015 Update:

The Corporation has deferred steps to resolve the prior year weaknesses, in light of the planned relocation to new office space in FY 2016. The CISO was reluctant to invest resources to upgrade the Corporation's existing network architecture prior to the move. According to the CISO, only 15-20 individuals in the Corporation utilize a "soft phone" connected to their laptop to make phone calls. The Corporation indicated that it plans to upgrade the Cisco Call Manager to resolve known security weaknesses with the installed version; however, the Corporation has not implemented an application firewall to limit the types of data traffic and network ports permitted to traverse from the data to the voice network. Limiting the types of network traffic permitted between the data and voice networks reduces the risk that the voice network could become unavailable due to a virus or denial-of-service (DOS) attack on the data network.

In subsequent discussions with the Corporation staff, they indicated their intent to secure the VoIP infrastructure by tasking their MITS vendor to perform a vulnerability assessment of the VoIP infrastructure and implementing additional access control restrictions between the data and VoIP virtual local area networks (VLAN).

FY 2014 Recommendations	FY 2015 Status
40. Review the VoIP configuration and restrict connectivity between the Corporation's data virtual local area network (VLAN) and voice VLAN to only those devices that must communicate with both VLANs. I. To restrict connectivity, consider implementing an application firewall to control network traffic to specific network protocols and ports between the data and VoIP VLANs. *(New for FY 2015)*	In Progress

[44] For full text of this prior year finding, please refer to page 36 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

41. Consider implementing the nine recommendations from NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, to improve the security over the Corporation's voice network.	In Progress
42. Consider contracting for a network penetration study and including the Corporation's voice network within the scope of the study.	In Progress
43. Determine if the legacy Cisco desktop application is still needed and remove it from all desktops and laptops if determined to be unnecessary.	In Progress
44. Correct factual inaccuracies in the system security plan for the Local Area Network (LAN)/Wide Area Network (WAN) regarding the Corporation's VoIP infrastructure and identify compensating controls to address the risks associated with commingling data and VoIP networks.	In Progress

Fiscal Year 2014 Finding #7: Lack of Segregation of Duties[45]

The Corporation has not completed documentation of SoD requirements for the eSPAN system. The same deficiency was reported in the FY 2013 FISMA evaluation and was first reported in the FY 2011 financial statement audit.

The Corporation has not met SoD compliance guidance as set forth by the NIST and OMB, such as NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Section AC-5: "Separation of Duties," that requires Federal organizations to document the SoD among individuals and define information system access authorizations to support SoD.

FY 2015 Update:

The Corporation has resolved the prior year weaknesses. Specifically, the Corporation has implemented a SoD Matrix for eSPAN to define the required SoD across all business processes and align this with its IT systems. The Corporation defined and documented the current process for system access management, showing the process and multiple approval layers. In conjunction with the system access management, the eSPAN SoD Matrix further identified the six sensitive roles (i.e., Program Officer, Senior Program Officer, Grants Officer, Senior Grants Officer, Executive Officer, and System Administrator) that pose the biggest threats for fraud and, accordingly, whose roles must be separated to certify, commit, and award funds to grantees.

FY 2014 Recommendation:	FY 2015 Status
45. Strengthen its controls surrounding SoD by documenting and maintaining a SoD Matrix for eSPAN that identifies the incompatible roles within the system. Specifically, the business process owners should work with the Office of Information Technology (OIT) to prioritize development of the SoD Matrix to identify where SoD violations could occur and restrict access accordingly.	Closed

[45] For full text of this prior year finding, please refer to page 39 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Fiscal Year 2014 Finding #8: Inadequate Incident Response Reporting[46]

The Corporation has not properly classified all computer security incidents, nor has it reported all computer security incidents to the United States-Computer Emergency Readiness Team (US-CERT).

NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, defines a computer security incident as, "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." To assist in incident handling, NIST SP 800-61, Revision 2, also identifies attack vectors, which can be used as a basis for defining more specific handling procedures. Theft and improper use are both reportable incidents in accordance with the NIST guidance. While an agency may have some latitude in reporting events to the public, there is no such latitude in reporting events to US-CERT.

FY 2015 Update:

The Corporation has resolved the prior year weaknesses. During FY 2015, the Corporation reported all incidents within the established US-CERT timeframes. Moreover, the Corporation recorded internal incident reports, such as the "Missing Information Technology (IT) Asset Form."

The Corporation's Incident Response Procedures now include the US-CERT Federal Agency Incident Categories Table, which offers a standardized policy that requires personnel to report incidents to US-CERT within a specific timeframe depending on the criticality of the event.

FY 2014 Recommendations	FY 2015 Status
46. Update the Corporation's Incident Response Plan to align with NIST SP 800-61, *Computer Security Incident Handling Guide*, and US-CERT guidance to properly classify and report computer security incidents.	Closed
47. Report all required security incidents to the US-CERT within the mandatory timelines.	Closed

[46] For full text of this prior year finding, please refer to page 41 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Fiscal Year 2014 Finding #9: Inadequate Enterprise-Wide Risk Management Policies and Practices[47]

The Corporation documented its risk management policies and security controls in its Information Assurance Plan (IAP) and in the respective SSP for its GSS and Major Applications (MA). However, these documents only described the risk management process at the information system (i.e., Tier 3)[48] level and discussed specific technical, management, and operational security controls focused at the Tier 3 level. Existing risk management processes do not address risks at Tier 1: *Organizational Perspective*[49] and Tier 2: *Mission/Business Process Level*.[50] The risk management practices largely did not involve the individuals who were responsible for accomplishing organizational, mission, and business objectives on a daily basis, such as the business owner or application owner. Thus, all risks may not be adequately considered and accounted for. Overall, the Corporation lacked a comprehensive and enterprise-wide Risk Management Program. This issue was previously reported in the FY 2013 FISMA evaluation.

NIST provides specific guidance to Federal agencies for implementing a Risk Management Program and supporting risk management practices. The Corporation has not implemented a comprehensive and enterprise-wide Risk Management Program, as required by several NIST SPs, including NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

[47] For full text of this prior year finding, please refer to page 43 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.
[48] Tier 3 risk management activities include: 1) categorizing organizational information systems; 2) 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; and 3) managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development life cycle process implemented across the organization.
[49] Tier 1 level risk management activities include: 1) the 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; 2) the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment; 3) the types and extent of risk mitigation measures the organization plans to employ to address identified risks; and 4) the level of risk the organization plans to accept (i.e., risk tolerance).
[50] Tier 2 level risk management activities include: 1) defining the mission/business processes needed to support the missions and business functions of the organization; 2) prioritizing the mission/business processes with respect to the strategic goals and objectives of the organization; 3) defining the types of information needed to successfully execute the mission/business processes, the criticality/sensitivity of the information, and the information flows both internal and external to the organization; 4) incorporating information security requirements into the mission/business processes; and 5) establishing an enterprise architecture with embedded information security.

FY 2015 Update:

In the FY 2013 and 2014 FISMA evaluations, Kearney reported similar weaknesses associated with the Corporation's risk management process. The Corporation has taken some steps, but with limited progress, to resolve the prior year weaknesses. The Corporation has documented the three tiers of management in the Enterprise Risk Management draft document to cover the enterprise level (i.e., Tier 1), the missions/business level (i.e., Tier 2), and the information systems level (i.e., Tier 3). Monthly IT Steering Committee meetings are held to make decisions concerning risks at the information systems level.

However, weaknesses remain with the Corporation's risk management and its policies and procedures. The Corporation did not assess risks for different business tiers as part of its SA&A process, or conduct business-owner risk surveys or similar risk assessments to identify new and potentially unknown risks. For example, the Corporation did not conduct a Business Impact Analysis (BIA), a Tier 2 risk assessment activity, to identify mission-critical business functions and quantify the impact of a loss if an underlying IT system is unavailable. In addition, the IAP, BIA, and Continuity of Operations Plan (COOP) need to be updated to address risks in Tiers 1 and 2 and to involve the system owners as part of the risk management process.

FY 2014 Recommendations	FY 2015 Status
48. Document and fully implement a comprehensive and enterprise-wide risk management process, that includes the following:	
a. Addressing and capturing risk at the organizational level (i.e., Tier 1), providing the context for all risk management activities carried out by the Corporation in order to understand where risk resides for prioritization of remediation strategies.	In Progress
b. Addressing and capturing risk at the mission/business process level (i.e., Tier 2), including clearly assigning ownership and responsibilities for executing risk management processes at this level.	In Progress
c. Integrating Tier 1 and 2 Level activities and linking them to Tier 3 Level activities related to implementation, operation, and monitoring of Corporation information systems.	In Progress
d. Integrating the risk management process with the Capital Planning and Investment Control (CPIC) process.	In Progress

Fiscal Year 2014 Finding #10: Weaknesses with the Corporation's Security Planning and Assessment Process[51]

The Corporation has outsourced its major information systems, such as its LAN/WAN GSS, eSPAN, and public-facing websites. As part of the contract requirements, the information system providers must be FISMA-compliant. However, the Corporation did not develop corporate standards for its multiple IT contractors to follow regarding ongoing security assessments and continuous monitoring activities, as mandated by OMB guidance and several NIST SPs, including NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The FISMA legislation of 2002 requires "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually."

FY 2015 Update:

The Corporation has taken steps and made some progress towards resolving the prior year weaknesses such as hiring a new CISO and a Security Analyst in June 2015. The Corporation also hired a contractor in May 2015 to support the Corporation's IAP and IT policy development. However, Corporation management stated that resource constraints precluded the Corporation from updating its SSPs and other documents prior to filling these vacancies.

In addition, the Corporation lacked consistent standards for SSPs and SARs across its multiple IT vendors. The Corporation did not correct errors and had incorrect references in its IAP and SSP for its Network GSS and MAs. The SSP in particular contained references to other documents, such as a "CNCS Service Account Approval and Tracking SOP" and "Wireless System Security Plan," but was unable to provide copies or other evidence that these documents existed. Implementation details for the various security controls and security control enhancements were inaccurate or outdated, reflecting that the annual review and update process by the IT contractor and Corporation was not effective.

Prior year conditions related to a lack of standard test cases to capture evidence of control effectiveness, promote re-use of tailored test cases, and ensure consistency across security control assessments were not developed in FY 2015. Further, the Corporation still has not developed a sampling plan for testing the operating effectiveness of controls, thus limiting the comparability between subsequent assessments, such as comparing continuous monitoring results between FYs 2014 and 2015. Finally, the Corporation did not document its approach for testing common controls or how the Corporation assesses required security controls that are not within the scope of the IT service provider's information systems, such as the Corporation's "common controls" and "privacy controls."

[51] For full text of this prior year finding, please refer to page 48 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Without clear standards and a structured approach for performing security control assessments, the Corporation's IT vendors may produce security assessment results of inconsistent quality and depth. Thus, the Corporation may not be fully aware of all the security risks.	
FY 2014 Recommendations	**FY 2015 Status**
49. Develop and implement a single security assessment process consistent with NIST SP 800-37, Revision 1, and NIST SP 800-53A for the Corporation's IT vendors to utilize.	In Progress
50. Establish security assessment standards, to ensure consistency and quality, such as:	
a. Sampling plan.	In Progress
b. Standard test cases.	In Progress
c. Determination of security assessor independence requirements.	In Progress
51. Review all NIST SP 800-53, Revision 4 security and privacy controls and allocate responsibility for implementing those controls to either the Corporation or its IT vendor for existing IT contracts.	In Progress
52. Assign responsibility for implementing specific NIST SP 800-53 security and privacy controls to either Corporation or the IT vendor prior to signing the contract. Incorporate the results of such analysis in the resulting IT contract to avoid ambiguity and subsequent vendor requests for a change order.	In Progress
53. Create a "Common Controls" security plan and privacy controls security plan for the security controls for which the Corporation will retain responsibility.	In Progress
54. Update the SSPs for eSPAN, Momentum, and LAN/WAN to ensure:	
a. SSP contains an accurate description of the information system and any sub-systems.	Closed
b. SSP clearly identifies the information system boundaries and technologies utilized within the boundary.	Closed
c. Responsibility for implementing each NIST SP 800-53 control is clearly delineated between the Corporation and IT vendor.	In Progress
d. SSPs accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls and required control enhancements.	In Progress
55. Strengthen oversight of the Corporation's IT contractors to ensure that: 1) all the SSPs are updated at least annually and are accurate, and 2) document its review of the SSP, SAR, and POA&M as part of the IT oversight process.	In Progress
56. Develop and implement an assessment approach for testing common and privacy controls that includes continuous monitoring aspects, such as the monitoring of audit logs, error reports, and performance metrics.	In Progress
57. Annually assess a subset of the Corporation's common controls and privacy controls.	In Progress

58. Complete Acceptance of Risk forms to formally evidence the Chief Information Officer (CIO) and business owner sign-off on risk acceptance. Electronically store the Acceptance of Risk in a central location so they may be readily searched during risk considerations.	In Progress

FY 2014 Finding #11: Lack of Formal Role-Based Training[52]

The Corporation has not implemented a formal, documented, role-based Information Security Training Program for all individuals with significant information security responsibilities (including regular training updates), as mandated by OMB guidance and as required by several NIST SPs, including NIST SP 800-16 and NIST SP 800-53, Revision 4. We have reported this issue since the FY 2013 FISMA evaluation. In FY 2014, the Corporation's MDCS (now MITS) contractor provided "Security Awareness and Incident Handling" training to employees on how to maintain a secure environment and collected acknowledgement of security responsibilities. However, training topics only covered general information security awareness and were not designed and targeted to different individual job functions. This awareness training does not meet the requirements of NIST SP 800-53, Revision 4 and NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* NIST SP 800-16 distinguishes between awareness and training and specifically states, "At the 'Training' level of the learning continuum, the specific knowledge and skills acquired may become obsolete as technology changes."

IT contractors for the Corporation's two major applications, Momentum and eSPAN, received no additional training beyond the general information security awareness training provided by the Corporation. In addition, the Corporation provided limited evidence of role-based training for certain individuals with significant information security responsibilities.

FY 2015 Update:

In the FY 2013 and 2014 FISMA evaluations, Kearney reported similar weaknesses associated with the Corporation's security training process. The Corporation has made limited progress towards resolving the prior year weaknesses. Privileged users at the Corporation and the MDCS contractor could not provide evidence of privileged user training, suggesting that training did not occur. The Corporation's MDCS contractor delivered the same generic training presentation on security awareness and incident handling, utilized in FY 2014, again in FY 2015. Similar to FY 2014, IT contractors for the Corporation's two major applications received no additional training beyond that offered by the Corporation. In addition, the Corporation provided limited evidence of role-based training for certain individuals with significant information security responsibilities. Similar to prior years, the individuals listed below with substantial IT responsibilities did not receive training commensurate with their job functions and responsibilities. These positions include:

- Corporation CIO
- Corporation Senior Security Consultant
- Corporation Project Manager
- Momentum Data Center ISSO
- Momentum Information Security Officer

[52] For full text of this prior year finding, please refer to page 56 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

- System Administrators (other than the GSS).

The Corporation's prior IT contracts and the new contract, MITS,[53] do not specifically require that IT contractors provide role-based security training for its employees serving the Corporation. For example, software developers are not required to complete any specific training on developing secure software. The Corporation has not required its IT vendors to demonstrate that employees serving the Corporation have completed annual specialized training. In addition, the Corporation's management stated that the awareness training provided to most IT employees is suitable for the agency's size and that it is not financially feasible to provide role-based security training to the number of individuals with significant information security responsibilities.

Finally, the Corporation did not deliver general user "awareness" training prior to September 30, 2015 and indicated its intent to conduct such awareness training in October 2015.

Subsequent to the completion of Kearney's fieldwork, the Corporation announced that it would hold live, in-person end-user security awareness training and conduct "Elevated Privileges Security Training" and "Role-Based Security Training" in October 2015 for Authorizing Officials (AO), Information System Owners (ISO), Information System Security Managers (ISSM), and ISSOs. When completed, these corrective actions should improve the Corporation's Information Security Program and address prior year recommendations.

FY 2014 Recommendations	FY 2015 Status
59. Enhance annual role-based information system security training for all employees with significant information security responsibilities to focus on technical areas relevant to a designated position, rather than awareness.	In Progress
60. Include contractual provisions requiring IT contractors to provide and document receipt of relevant annual IT information system security training for contractor employees with significant information security responsibilities.	In Progress
61. Maintain evidence of security training for the Corporation's employees and IT contractors with significant information security responsibilities.	In Progress

[53] See related FY 2015 new FISMA finding: *Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses.*

Fiscal Year 2014 Finding #12: Improvements Needed to POA&M Reporting[54]

The Corporation did not have an adequate POA&M management process in place to ensure that all known security weaknesses are recorded, resources needed for remediation are identified, and progress toward timely resolution is adequately monitored. The Corporation's POA&Ms did not identify resources required to resolve open tasks, such as estimating the level of effort in man-hours or other costs to procure contractor support or tools. Such requirements for the POA&M management process are mandated by the OMB guidance and NIST SPs, including NIST SP 800-65 *Integrating IT Security into the Capital Planning and Investment Control Process,* and NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*.

FY 2015 Update:

In the FY 2013 and 2014 FISMA evaluations, Kearney reported similar weaknesses associated with identifying required resources with the Corporation's POA&M management process. The Corporation has taken some steps, but with limited progress, to resolve the prior year weaknesses. The Corporation instituted an additional corporate-level POA&M to track the progress of prior year FISMA findings, began quarterly POA&M reviews, and established a new POA&M format. The Corporation has prepared a draft SOP for POA&M management, which is designed to assist ISSOs/Information System Security Managers (ISSMs), ISOs, and supporting OIT staff in identifying, assessing, prioritizing, monitoring, and routinely reporting on the progress of corrective actions taken to remedy security weaknesses. In addition, the Corporation has issued a POA&M policy document detailing guidance and reporting requirements to all system owners. The CIO reported that the Corporation is in a better position to hold system owners accountable, as OIT requires system owners to set specific milestone dates, identify delays, and provide revised completion dates to maintain a log for each individual POA&M items.

However, weaknesses remain related to the Corporation's POA&M process. The Corporation's outsourcing strategy requires that its contractors maintain a POA&M for their respective information systems. Thus, security weaknesses spanning across multiple information systems were not captured until the Corporation implemented a new POA&M process in March 2015.

Further, the Corporation's POA&M guidance requires that the ISSO and ISO identify resources required to resolve POA&M items and establish completion dates. However, based on the May 15, 2015 corporate-level POA&M, none of the 60 open POA&M items specified the resources required for issue resolution, and 56 of the 60 POA&M items lacked a scheduled remediation date.

In addition to omitting resource requirements and scheduled remediation dates for entity-level PO&AM items, similar weaknesses existed for the Corporation's 10 information system-level

[54] For full text of this prior year finding, please refer to page 60 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

POA&Ms, which included missing resources (i.e., technical or work hours), estimated resolution costs, and milestone completion dates.	
FY 2014 Recommendations	**FY 2015 Status**
62. Enhance the POA&M process to identify resources required for remediation in either the POA&M item or associated change request ticket.	In Progress
63. Establish a Corporation-wide Information Security Program POA&M to track security issues that are broader than a single information system, such as findings from management studies like the MITRE report or annual OIG FISMA evaluations; as part of this process, the Corporation should turn broad risks into recommendations that are actionable and able to be included and tracked on a POA&M.	Closed
64. Document acceptance of risk for items that will not be remediated, along with planned mitigating controls.	In Progress
65. Strengthen the POA&M management process by: 1) developing detailed instructions for documenting POA&M items; 2) formally assigning responsibility for tracking and regularly updating all POA&Ms; 3) including all known security weaknesses, including low and moderate; and 4) establishing performance metrics or practices to communicate, semi-annually or annually, to the Corporation's Chief Executive Officer (CEO) or Chief Operating Officer (COO) on known security weaknesses and associated resource needs to coincide with budget requests.	In Progress

Fiscal Year 2014 Finding #13: Inadequate Controls Over Remote Access[55]

Corporation-issued laptops were configured to connect automatically to the Corporation's network through Cisco's "AnyConnect Virtual Private Network (VPN)" client. However, the automatic connection of the laptop to the VPN server does not meet the two-factor authentication requirements for Federal agencies where "one of the factors is provided by a device separate from the computer gaining access." In addition, the Corporation incorrectly configured its VPN to permit the use of non-compliant Federal Information Processing Standards (FIPS) Publication (PUB) 200 encryption algorithms and network protocols, leaving VPN sessions vulnerable to exploitation. The related criteria are required by OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, and NIST SPs, including NIST SP 800-52, Revision 1, *Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations*.

FY 2015 Update:

The Corporation has taken some steps, with limited progress, to resolve the prior year weaknesses; it has initiated, but not completed, adoption of two-factor authentication using a Personal Identity Verification (PIV) card. In light of recent security breaches at other Federal agencies, the CIO stated that the Corporation has made funding request in its FY 2017 budget for the implementation of two-factor authentication and as part of an unfunded budget request for FY 2016.

During FY 2015, the Corporation adjusted its VPN device configuration to accept only Transport Layer Security (TLS) v 1.0 protocol connection requests rather than Secure Socket Layer (SSL) v 3.0 requests, which is not FIPS PUB 200 approved. TLS is a protocol created to provide authentication, confidentiality, and data integrity between two communicating applications, such as a VPN network device and a VPN client on a laptop. TLS protocol is based on the precursor protocol SSL 3.0 and corrects security weaknesses in SSL 3.0. TLS also protects application data traversing a network by using a set of cryptographic algorithms. Under the FISMA legislation of 2002, NIST requires that Federal agencies use only approved cryptographic algorithms for key exchange, encryption, and message integrity. Thus, the Corporation must only use cryptographic algorithms in its VPN device and protocols that are federally approved by NIST. As security weaknesses are constantly discovered with VPN software and cryptographic algorithms, the Corporation must closely monitor vendor announcements for software fixes to correct security weaknesses in its VPN network device and VPN client software.

In July 2015, Kearney noted that the Corporation did not operate the current version of the Cisco VPN software for its VPN network device and was using unapproved protocols and cryptographic algorithms. Further, the cryptographic algorithm used for message integrity, called the Secure Hash Algorithm (SHA), was SHA-1, which was not the approved versions of

[55] For full text of this prior year finding, please refer to page 63 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

SHA-2 or SHA-3. NIST SP 800-52, Revision 1, Section 3 states, "TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended." Subsequently, on August 5, 2015, NIST announced that Federal agencies should use SHA-3 cryptographic hash function[56] to correct recently discovered security weaknesses in SHA-1. As of July 2015, both the TLS 1.2 protocol and SHA-2 cryptographic algorithm were available in the current release of the Cisco VPN software. However, the Corporation had not deployed the current software version on its VPN network device at the time of Kearney's testing conducted in July 2015.

The Corporation conveyed that its current VPN device was unable to support the latest version of TLS 1.2 and would require a hardware upgrade. Accordingly, the Corporation has requested that its MITS vendor upgrade the VPN hardware to support the federally approved protocols and cryptographic algorithms.

FY 2014 Recommendations	FY 2015 Status
66. Review and update the hardware and/or configuration of the SSL/TLS VPN device to comply with FIPS PUB 140-2- and FIPS PUB 202-approved cryptographic algorithms (i.e., 3DES, AES-128, AES-256, ~~SHA-1*~~, SHA-2, and SHA-3) and TLS 1.2. (**Kearney revised this recommendation to remove the SHA-1 reference as NIST removed SHA-1 from its approved list of cryptographic algorithms in August 2015 due to known weaknesses.)*	In Progress
67. Implement a VPN solution that complies with OMB Memorandum M-06-16 and NIST SP 800-53, Revision 4, mandatory security controls for Federal agencies by using multi-factor authentication.	In Progress
68. Strengthen oversight of MDCS contractors to ensure proper implementations of IT products and timely installation of vendor-supplied patches, and, as necessary, develop a formal, documented risk acceptance process to include establishment of mitigating controls.	In Progress

[56] FIPS PUB 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, dated August 2015, establishes the new requirement to use a more secure hashing algorithm.

Fiscal Year 2014 Finding #14: Inadequate Disaster Recovery Plan Documentation and Planning[57]

The Corporation's DRP does not include all of the Corporation's essential functions and missions. The BIA specifically stated that it is not meant to address all essential business functions and refers to the Corporation's COOP and DRP for coverage. However, neither the COOP nor the DRP addresses all essential business functions. Further, the Corporation's DRP was written specifically for MDCS; it is not representative of the Corporation as a whole and did not acknowledge other key IT contractors and systems. Based on review of available BIAs, DRPs, and COOP documentation, the Corporation had a gap in its COOP and consideration of essential business functions.

FY 2015 Update:

The Corporation did not make progress to resolve weaknesses associated with the Corporation's DRP documentation and planning. Kearney noted that the Corporation relies on the MITS DRP to cover the entire agency; however, the DRP, which focuses on MITS systems, does not encompass all critical business functions needed to provide an adequate COOP for the entire Corporation. In addition, there is no contractual requirement for annual DRP testing in the new MITS contract and Corporation management has not prioritized annual disaster recovery testing.

In addition, the Corporation did not conduct a BIA to identify organizational risks that should be addressed in the COOP, nor develop an agency-wide COOP, a GSS DRP, and a financial system Contingency Plan. The Corporation provided Kearney a draft COOP; however, the Corporation did not follow guidance per the NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, that states the "COOP should not be completed without a completed BIA."

FY 2014 Recommendations	FY 2015 Status
Kearney recommends that the Corporation develop a more effective and comprehensive DRP and COOP by:	
69. Developing an individual BIA for each critical system with participation from the business owner.	In Progress
70. Determining information system recovery criticality, including allowable downtime and acceptable data loss based on business process needs.	In Progress
71. Identifying outage impacts, resource requirements, and recovery priority for system resources.	In Progress
72. Updating the DRP to cover the entire Corporation and other critical IT contractors and not just the MDCS.	In Progress
73. Updating the COOP based on revisions to the BIA and DRP.	In Progress

[57] For full text of this prior year finding, please refer to page 67 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation* for FY 2014.

Fiscal Year 2014 Finding #15: Opportunities to Strengthen Continuity of Operations Planning and Testing[58]

The Corporation did not conduct adequate planning or testing of its COOP. The following aspects of the Corporation's COOP and DRP made it inadequate:

- The COOP did not include sufficient information to address all mission-essential functions and subordinate plans and details that would be necessary should the plan ever need to be activated
- The Corporation made assumptions that did not appear reasonable should it be necessary to activate the COOP, such as all vital records being available electronically and all employees who support essential business functions having laptops
- Evidence of annual COOP testing, including after-action reports, as required for mission-essential functions and the agency's financial system, did not exist.

The Corporation did not follow NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, which states, "Testing should occur based on organization requirements and when significant changes are made to the information system, supported mission/business process(s), or the ISCP. Each element of the ISCP should be tested first individually and then as a whole to confirm the accuracy of recovery procedures and the overall effectiveness."

FY 2015 Update:

The Corporation did not make progress to resolve weaknesses associated with the Corporation's COOP planning and testing. The Corporation did not conduct or update its BIA in FY 2015 to identify organizational risks that should be addressed in the COOP, nor has it developed an agency-wide COOP, a GSS DRP, and a financial system Contingency Plan. The Corporation provided us a draft COOP; however, the draft documents suggested the Corporation did not follow guidance per NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, which states, "the COOP should not be completed without a completed BIA." Further, the Corporation did not test its COOP at all in FY 2015.

In addition, the responsibility for COOP was assigned to the COOP Executive Team (CET), placing control under the purview of multiple individuals, as opposed to a central individual. The number of individuals involved may lead to confusion in the event of required COOP activation.

Kearney also noted that the Corporation relies on the MITS DRP to cover the entire agency; however, the DRP, which focuses on MITS systems, does not encompass all critical business functions needed to provide an adequate COOP for the entire Corporation.

[58] For full text of this prior year finding, please refer to page 70 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Subsequent to the completion of Kearney's fieldwork in August 2015, the Corporation reported that it is in the process of identifying the stakeholders for mission/business functions enterprise-wide to complete the BIA and update the COOP and DRP. This effort will also enable documentation of mission-essential functions, including the IT components that support these processes, and the recovery procedures needed in the case of a contingency or disaster. The Corporation also stated that it plans to implement and document annual COOP exercise and document and share the lessons learned from these exercises.	
FY 2014 Recommendations	**FY 2015 Status**
74. Define a clear chain of command to clarify responsibilities and identify an ISCP Director to oversee Corporation-essential functions regarding the COOP.	In Progress
75. Review the assumptions that are included in COOP documentation and ensure that the assumptions are valid and realistic.	In Progress
76. Update the COOP documentation to ensure that all mission-essential functions are considered and have detailed plans for resumption of operations.	In Progress
77. Conduct a COOP test at least annually and capture lessons learned in a formal after-action report.	In Progress

Fiscal Year 2014 Finding #16: Inadequate Controls over Privacy Data[59]

The Corporation did not explicitly document its privacy controls, as required by Appendix J: *Privacy Controls* of NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Other weaknesses associated with the Corporation's Privacy Program included:

- The Corporation did not fully document its PII inventory
- Corporation employees did not comply with requirements to destroy outdated records containing PII in accordance with the Record Retention Schedule promulgated by NARA
- The Corporation did not update and publicly post the Privacy Impact Assessments (PIA) for two key information systems, Momentum or eSPAN, since 2009.

FY 2015 Update:

The Corporation has taken some preliminary steps to establish conditions necessary to address the prior year weaknesses. These steps include hiring a new CISO and a Security Analyst in June 2015 and hiring a contractor in May 2015 to support the development of the Corporation's Information Security Program. Additionally, the Corporation also stated its intent to appoint an individual outside of the Office of Information Technology (OIT) as the Chief Privacy Officer. Furthermore, the Corporation has prepared an initial version of its Privacy Controls Implementation Plan (Appendix J of NIST SP 800-53) to document the organizational controls for protecting privacy and PII within the Corporation's systems. However, Kearney noted factual inaccuracies within the Privacy Controls Implementation Plan. The Corporation should also further improve the usefulness of the Privacy Controls Implementation Plan by describing how privacy controls are implemented and identifying the responsible party for implementing operational aspects, such as maintaining and periodically updating the Corporation's PII inventory, as well as individuals responsible for preparing and posting Privacy Impact Assessments (PIA) and System of Records Notices (SORN) for new IT systems collecting PII from the public.

As part of our procedures to evaluate the Corporation's implementation of privacy controls, Kearney performed site visits at the Field Financial Management Center (FFMC), Philadelphia State Office, Maryland State Office, and National Civilian Community Corps (NCCC) Baltimore Campus. Our site visits disclosed that some of the Corporation's employees did not follow NARA Record Retention Schedule requirements for records containing PII and dispose those records once the expiration date passed. This finding has been repeated for the last three consecutive years during our site visits at various Corporation locations. In addition to retaining unnecessary records containing PII, Kearney observed another instance involving unsecured PII at the Corporation's headquarters. Kearney observed two boxes of mail, with the Corporation program members' addresses and other PII clearly visible through the envelopes' address windows, was left unattended in an unsecured hallway in front of the United States Postal

[59] For full text of this prior year finding, please refer to page 73 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

Service (USPS) mailbox. As individuals continue to retain records containing PII beyond the statutory period or fail to secure PII information properly, Kearney concluded that the Corporation's privacy training, policies, and procedures related to PII storage were not fully effective.

Additionally, the Corporation did not update the PIAs for two major IT systems, Momentum and eSPAN, although we noted this issue for previous years. Finally, the Corporation has not officially designated a Chief Privacy Officer (CPO).

FY 2014 Recommendations	FY 2015 Status
78. Update, document, and implement the privacy controls required by Appendix J of NIST SP-800-53, Revision 4, and perform continuous monitoring, as necessary, to comply with the provisions of the publication.	In Progress
79. Re-evaluate the sufficiency of resources to implement required privacy controls and ensure an individual is identified and assigned responsibility for these privacy controls.	In Progress
80. Fully document information contained in the PII Tracking Sheet as part of improving the process to minimize the use, collection, and retention of PII.	In Progress
81. Ensure Corporation staff are aware of, and comply with, NARA retention requirements for maintaining physical PII records.	In Progress
82. Update the PIAs for Momentum and eSPAN and post them (redacted of sensitive security information) on the Corporation's public website in accordance with Section 208 of the e-Government Act.	In Progress
FY 2015 New Recommendations	
II. Designate a Chief Privacy officer to ensure an individual is identified and assigned responsibility for privacy controls	New
III. Enhance security training for all employees to address awareness of PII and records management security.	New

APPENDIX C: MANAGEMENT'S RESPONSE

Corporation for NATIONAL & COMMUNITY SERVICE

1201 New York Avenue, NW
Washington, DC 20525
202-606-5000
NationalService.gov

TO: Stuart Axenfeld
Office of the Inspector General (OIG)

FROM: Jeffrey Page
Chief Operating Officer

SUBJECT: Request for Comments on the OIG Draft Report: Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2015

Date: November 11, 2015

This memorandum responds to your email on this subject, dated October 30, 2015.

The Corporation for National and Community Service (CNSC) appreciates the opportunity to review the draft report and offers the following general comments. More detailed comments and actions planned in response to specific OIG findings and recommendations are attached.

CNCS is committed to maintaining a strong and effective Cybersecurity Program. Effective Cybersecurity enables CNCS to meet our responsibilities to our members, grantees and others who trust us to protect the personally identifiable information (PII) they share with us. During 2015, CNCS has made steady improvements to the overall Cybersecurity program.

During FY 2015, all vacant Cybersecurity positions were filled and a contract was awarded to provide the support required to address the OIG's 2014 recommendations. While much more progress was made in resolving findings than is acknowledged in this FISMA report, we understand that this is a function of the period the audit covers, and we are now focused on resolving the remaining findings and recommendations of the OIG evaluation team. We consider these findings and recommendations to be extremely useful in improving the Cybersecurity Program. We will continue to place a high priority on addressing them in a timely and effective manner.

During FY 2015, we developed a plan to address all Cybersecurity issues. This plan is a multi-year plan that will put CNCS in the best position to succeed in the future. CNCS has established a FISMA Remediation Team that meets monthly to monitor the progress that is being made in addressing the Cybersecurity issues. We continue to work with DHS on the implementation of their programs and services for CNCS, including Risk and Vulnerability Assessments, the Cyber Hygiene Program, and Continuous Diagnostics and Mitigation – all important parts of a strategic Information Security Continuous Monitoring approach.

We believe that a Cybersecurity Program-wide response is the most appropriate strategy to addressing the issues identified by the OIG, rather than developing point solutions for specific findings. The FISMA recommendations will be incorporated into the agency's overall Plan of Actions and Milestones (POA&M) documentation.

As communicated during the evaluation, Cybersecurity training was completed during October for general users, elevated privileged users, and users with security roles. We achieved 100% compliance by October 31, 2015, the earliest and most successful security training that the agency has ever conducted. In summary, CNCS will continue to work diligently to implement the Cybersecurity Program improvements. Operational considerations will require that CNCS phase in changes over time and in the case of DHS involvement, adhere to the schedule that is being dictated. Some fundamental improvements will extend beyond FY 2016 for full implementation. CNCS invites the OIG to participate on a regular basis in agency Cybersecurity Program planning and implementation reviews and to offer feedback as the improvement program unfolds.

If you have any questions regarding these comments on the OIG's draft FISMA evaluation report, please contact Jeffrey Page, CNCS COO at 202-606-6632, or Tom Hanley, CNCS CIO at 202-606-6618.

Attachment

Agency Comments on the OIG Draft Report: Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2015

cc: Thomas R. Hanley, Jr., Chief Information Officer
Guy Hadsall, OIG Chief Technology Officer

CNCS Comments on the OIG Draft Report:

Per the 2014 CNCS FISMA Report and OMB Memorandum M-14-04, the definition of "Significant Deficiency" is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and other agencies must be notified and immediate or near-immediate corrective action must be taken.

Since the issuance of the FY 2014 FISMA Report, CNCS has made marked improvements to its overall security posture; per this definition, the agency believes that several of the Significant Deficiency severity ratings should be reduced to Control Deficiency, specifically the NFRs grouped under Continuous Monitoring and Risk Management. Details demonstrating progress are identified in our responses to each findings category below.

Agency Response to Kearney Reported FY 2015 New Findings and Recommendations:

CNCS Response to "Inadequate Planning and Untimely Award of Information Technology (IT) Contract Delays Remediation of Information Security Weaknesses"

CNCS partially concurs with the findings that were disclosed in this document. It should be noted that the agency took what it deemed to be the proper steps in releasing the Managed Information Technology Services (MITS) contract. The SOW was distributed to approximately 20 vendors that had specific qualifications in the area of Data Center / IT Service solutions. Additionally, options for awarding through a Government Wide Acquisition Contract (GWAC) were researched. The agency made a determination that the hosting was not a core service on the CIOSPIII GWAC, the vehicle the agency was most familiar with, and after a review of pricing from other agencies, cross servicing costs were out of line with what we believed to be reasonable. Furthermore, while the agency did not receive the response that we had hoped for, the re-issuing of the solicitation would have caused further delays in making the award. The agency received a successful bid; therefore there was no justification to re-issue the RFP.

The CNCS Cybersecurity team did not believe at any time that the PII and sensitive data that was entrusted to the agency was at risk due to the procurement delays.

SLAs were provided as part of the RFP response from the contractor that received the award. The proposed service levels have been accepted by the government with the understanding that during the transition period, the government will be assessing and evaluating those SLAs and adjustments will be made as part of the transition effort under the MITS contract.

The Office of Information Technology has shared these recommendations with the new Director of the Office of Procurement Services for a determination as to what actions to take. Appropriate actions are already underway within OIT related to recommendation #2.

CNCS Response to "Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement"

CNCS agrees with the findings and recommendations in this report. While the agency may not agree with the reported status of all of the accounts in the enclosed table, this review brought to light several areas where account management could be strengthened. With the implementation of the new Off-Boarding system, user separation information has proven to be more accurate and timely; however, we have identified additional areas for improvement and will make adjustments to both policies and procedures, accordingly.

CNCS Response to "Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan"

CNCS agrees with the findings and recommendations in this report. The agency is in the process of reviewing and updating the CNCS IT Strategic Plan to:

1. Including current IT modernization efforts and future IT investments.
2. Updating performance metrics to measure success and determine if milestones are being achieved.
3. Defining roles and responsibilities of identified human resources.
4. Periodically updating the Plan to reflect major changes in IT strategy.

The agency is in the process of developing an agency Enterprise Architecture Plan (EAP) that will highlight the agency's current IT Modernization efforts. The plan will define the types of data, applications, hardware, and software that support the organization's network architecture. The plan will be reviewed annually, and updated as needed.

CNCS Response to "Inaccurate Inventory of Physical Information Technology (IT) Assets"

CNCS partially concurs with the findings that were disclosed in this document. This review brought to light several areas where the Inventory of Physical Information Technology Assets could be strengthened, although CNCS feels it would be cost prohibitive at this time for CNCS to perform a biannual physical inventory for HQ and all field offices, as CNCS plans to add more locations soon. CNCS plans to update the inventory, inventory SOP, and inform field offices of the more stringent requirements.

Agency Response to Kearney Reported Resolution Status of FY 2014 Notice of Findings and Recommendations:

FY 2014 FISMA Reporting Area Summary of NFRs	FY 2013 Repeat Finding	FY 2014 Severity	FY 2015 Status	FY 2015 Severity
Continuous Monitoring Management				
1. Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy	X	Significant Deficiency	In Progress	Significant Deficiency
2. Multiple Weaknesses with Vulnerability Scanning and Remediation		Significant Deficiency	In Progress	Significant Deficiency
3. Organizational Conflict of Interest		Significant Deficiency	In Progress	Significant Deficiency
4. Use of an Obsolete and Unsupported Network Monitoring Tool		Significant Deficiency	In Progress	Significant Deficiency
Configuration Management				
5. Lack of Controls to Prevent Use of Unauthorized Devices		Control Deficiency	Done	N/A
6. Risks to the Confidentiality and Availability of Voice Communications		Control Deficiency	In Progress	Control Deficiency
Identity and Access Management				
7. Lack of Segregation of Duties (SoD)		Control Deficiency	Done	N/A
Incident Response and Reporting				
8. Inadequate Incident Response Reporting		Control Deficiency	Done	N/A
Risk Management				
9. Inadequate Enterprise-Wide Risk Management Policies and Practices	X	Control Deficiency	In Progress	Control Deficiency
10. Weaknesses with the Corporation's Security Planning and Assessment Process	X	Significant Deficiency	In Progress	Significant Deficiency
Security Training				
11. Lack of Formal, Role-Based Training	X	Control Deficiency	In Progress	Control Deficiency

FY 2014 FISMA Reporting Area Summary of NFRs	FY 2013 Repeat Finding	FY 2014 Severity	FY 2015 Status	FY 2015 Severity
Plans of Action and Milestones (POA&M)				
12. Improvements Needed to POA&M Reporting	X	Significant Deficiency	In Progress	Control Deficiency
Remote Access Management				
13. Inadequate Controls over Remote Access		Control Deficiency	In Progress	Control Deficiency
Contingency Planning				
14. Inadequate Disaster Recovery Plan (DRP) Documentation and Planning		Control Deficiency	In Progress	Control Deficiency
15. Lack of Adequate Testing of Continuity of Operations Plan (COOP)		Control Deficiency	In Progress	Control Deficiency
Privacy				
16. Inadequate Controls over Privacy		Significant Deficiency	In Progress	Control Deficiency

CNCS Continuous Monitoring Management Response:

Senior executives and subject specific committees meet on a regular schedule and identify potential risks that need to be addressed at the Tier 1, Tier 2, and Tier 3 levels. CNCS is currently receiving Department of Homeland Security (DHS) Continuous Diagnostics and Monitoring (CDM) services, including Einstein 1 and 2 (E1 and E2) tool scan results along with Managed Trusted Internet Protocol Services (MTIPS) via Verizon. CNCS takes action based on these results. The MTIPS tool sits on the CNCS boundary and provides additional alerting and protections to CNCS; MTIPS will end a session/connection if it appears harmful. The MTIPS reports are received by CNCS Cybersecurity, including the CISO. CNCS signed the MOU with DHS on November 13, 2014 for DHS's continuous monitoring, management, and support services to include E3 intrusion prevention system (IPS). DHS is unable to provide these services until it receives its related funding, which is expected to occur in FY 2016.

The CNCS draft Enterprise Risk Management Policy (ERMP) was provided to the auditor on August 25, prior to the end of the assessment period.

Prior to the award of the Managed Information Technology Services (MITS) contract to SRA, scanning for vulnerabilities was placed under a regular schedule in March 2015 and documented for review. Vulnerability scan reports are reviewed, and the findings are discussed during weekly operations meetings that include CNCS Cybersecurity. The SRA

weekly operations report have included information from the DHS weekly Hygiene Reports (since January 2015) and E1 MTIPS reports from Verizon. Status based on McAfee Vulnerability Manager (MVM) reports have been included since March 2015. The MTIPS reports are received by CNCS Cybersecurity, including the CISO.

In FY 2015 Q2, POAM reporting was significantly strengthened, and the required reporting is completed quarterly.

OIT is working towards finalizing the ISCM strategy and the draft ISCM document.

SRA manually downloads McAfee updates that usually include Foundstone patch for MVM Version 7.5, FSL Scripts, Language pack, McAfee SCAP Content, O/S Fingerprints, and Threat Intelligence. Updates are manually installed weekly to ensure patches are all applied on a monthly patch cycle or earlier, depending on the severity of the vulnerability.

The MITS contract includes clauses to ensure SRA meets network and application security and privacy data protection requirements, including those of FISMA, NIST, OMB, NARA, and CNCS, with contract termination as a possible penalty for noncompliance. (See Sections 1.2 to Section 1.5 for details). Included are requirements for vulnerability and incident reporting and investigation support; appointment of an Information System Security Officer; compliance to network and application security baselines including those of United States Government Configuration Baseline (USGCB), NIST National Checklist Program Repository; data compartmentalization; and guaranteed CNCS access to the contractors' "facilities, installations, operations, documentation, databases, and personnel" to audit compliance to these requirements.

The Continuing Resolution (CR) prevented the hiring of VMD System Integrators staff from coming on board any earlier than May 2015. This staff is in place to support the Cybersecurity Program.

Audit logging via the Cisco Security Monitoring, Analysis, and Response System (MARS) tool is occurring while CNCS configures the USGCB and SCAP compliant Nessus tool. Nessus deployment is expected in December 2015.

CNCS proposes that this progress justifies a reconsideration of the rating of "Significant Deficiency" to "Control Deficiency".

CNCS Configuration Management Response:

Cisco port security restricts the MAC address and VLAN allowed on any given access port. Role based access controls are in place to allow only administrators of a computer to inspect traffic from its directly connected phone for troubleshooting purposes; no sensitive data are revealed on the read only phone statistic pages.

CNCS has taken several steps, some before the end date of this audit, to address separation of data and Voice over Internet Protocol (VoIP)) networks in compliance to NIST Special Publication (SP) 800-58, *Security Considerations for Voice Over IP Systems*:

- The MITS network support contractors are required to implement secure compartmentalization of data, in part to improve separation of data from voice communications (Voice over Internet Protocol (VoIP)), via Section 1.4 System Security Requirements, of its contract with CNCS.
- CNCS has an active contract for implementing new versions of Cisco Unified Communication Manager (CUCM), VoIP gateway, and telephone stations.
- VoIP tasks assigned by CNCS to SRA indicate the contractor will "Perform a vulnerability assessment and any required system hardening for VoIP gateways." The Information Systems Security Officer indicated SRA is following the recommendations in NIST Special Publication 800 58 - *Security Considerations for Voice Over IP Systems* where applicable. Voice VLAN access controls, including ICMP ping and HTTP access to phone statistics, will be reconsidered during the system hardening phase. This hardening effort is in progress and will continue as part of the relocation of the Agencies Headquarters specifically to establish access controls between both voice and data VLANS.
- System Security Plan (SSP) updates have been made to correct information on the Local Area Network (LAN)/Wide Area Network (WAN) regarding the Corporation's VoIP infrastructure. Compensating controls to address the risks associated with commingling data and VoIP networks have been described, and the configuration improvement and software upgrade efforts have been described.

CNCS Risk Management Response:

In FY 2015 CNCS has hired a new CISO, a Security Analyst, and a contractual security staff (VMD System Integrators) to implement FISMA-compliant security assessments and authorization efforts to include updating and standardizing its SSPs, as well as other CNCS cybersecurity related policies and procedures, and to ensure a structured approach for performing security control assessments. These CNCS and contractual personnel have been in place since May of 2015. Such actions constitute significant progress toward building a cybersecurity department capable of implementing FISMA-compliant SA&A documentation and practices.

With this new level of support, CNCS has made significant progress in drafting and finalizing its enterprise-level policy and procedure documentation:

- CNCS provided a final draft of the Enterprise Risk Management Policy (ERMP) document that addresses risk management at the enterprise level (i.e., Tier 1), the missions/business level (i.e., Tier 2), and the information systems level (i.e., Tier 3). IT Steering Committee meetings are held to capture and address risks at the information systems level.
- During the audit, the COOP was updated and signed. In September 2015, this COOP was exercised as the entire agency teleworked for 3 days. OIT has recommended reestablishing formal yearly testing as part of the government-wide Eagle Horizon

exercises. The COOP identifies a COOP Coordinator. The coordinator contacts managers who make the decision to activate the COOP. CNCS is discussing designation of one contact responsible for activating the COOP.

- The CNCS Capital Planning and Investment Control (CPIC) policy was updated and is awaiting signature. The CPIC is in accordance with guidance and requirements of the Office of Management and Budget (OMB) and Clinger-Cohen Act (CCA) and meets objectives that include the following:
  - Align IT Investments with business strategies, initiatives, and priorities
  - Coordinate and maximize the benefits from IT investment across the agency, regardless of funding sources
  - Manage risk effectively to deliver responsive, reliable, cost-effective IT services to the agency
  - Meet the CPIC requirements established by CCA.

  The CNCS CPIC policy requires that CPIC processes "…integrate with other IT management processes including information security, privacy, and accessibility."
- A Business Impact Assessment (BIA) is in place, and CNCS is identifying the stakeholders for discussions on Tier 2 mission/business priorities and risk.
- The Cybersecurity Policy (referred to earlier as the Information Assurance Policy (IAP)) draft was presented to Cybersecurity for review in October 2015.

In addition, an Integrity Steering Committee (Tier 2) meets to identify risks to CNCS and discuss remediation and/or mitigations needed to reduce or eliminate these risks. A meeting on July 23, 2015, included a review of the findings of this audit and actions taken to resolve the issues identified.

CNCS proposes that this progress justifies a reconsideration of the rating of "Significant Deficiency" to "Control Deficiency".

CNCS Security Training Response:

CNCS provided online computer security awareness training for all CNCS users before September 30, 2015. CNCS is providing the computer security awareness training via live seminars, after which all CNCS employees and contractors are required to attend and sign an updated Rules of Behavior (ROB). CNCS Cybersecurity is conducting three security trainings: Elevated Privileges Security Training, Role-Based Security Training, and CNCS Cybersecurity User Training. Cybersecurity Role-Based Training must be completed by Authorizing Officials (AO), Information System Owners (ISO), Information System Security Managers (ISSM), and Information System Security Officers (ISSOs). The Cybersecurity SharePoint (intranet) site is being updated, and all security trainings will be required and made available via that site. A workflow has been created to track completion of these required security trainings.

CNCS Plans of Action and Milestones (POA&M) Response:

CNCS has taken numerous actions to implement and formalize its POA&M procedures at all levels of the organization. The auditor states that CNCS "instituted an additional corporate-level POA&M to track the progress of prior year FISMA findings, began quarterly POA&M reviews, and established a new POA&M format. The Corporation has updated a draft SOP for the POA&M, which is designed to assist ISSOs/Information System Security Managers (ISSMs), ISOs, and supporting OIT staff in identifying, assessing, prioritizing, monitoring, and routinely reporting on the progress of corrective actions taken to remedy security weaknesses. In addition, the Corporation has issued a POA&M policy document detailing guidance and reporting requirements to all system owners. The CIO reported that the Corporation is in a better position to hold system owners accountable, as OIT requires system owners to set specific milestone dates, identify delays, and provide revised completion dates to maintain a log for each individual POA&M items." Enterprise-level POA&M items were captured even before May 2015, when the new CISO, Security Analyst, and cybersecurity contractors began. The auditor acknowledges also that "security weaknesses spanning across multiple information systems were… captured [when] the Corporation implemented a new POA&M process in March 2015."

CNCS Remote Access Management Response:

CNCS has implemented personal identity verification (PIV) cards for a limited number of CNCS employees. Full implementation is being planned for and the necessary funding for two-factor authentication via PIV cards has been included as part of the OIT budget request for FY 2017.

Implementation of a more recent version of Security Sockets Layer (SSL) encryption is in progress for network traffic until Federal Information Processing Standards (FIPS) compliant Transport Layer Security (TLS) can be implemented. The configuration of the current hardware that is in production is unable to support TLS 1.2 due to firmware limitations. Upgrades to the current hardware are planned as part of the MITS transition and should be completed by Q2 FY 2016.

CNCS Contingency Planning Response:

CNCS finalized and signed an enterprise-wide COOP September 2015. CNCS plans to implement and document annual exercises of the COOP and document and share the lessons learned from these exercises (as part of Eagle Horizon).

The CNCS MITS contract with SRA was finalized and signed in July 2015. This contract includes in Section 2.2, Applicable Documents, Item 22, "Information System Contingency Plan" document as a requirement.

CNCS is identifying the stakeholders for mission/business functions enterprise-wide to complete the BIA and update the COOP and DRP. This effort will also enable documentation of mission-essential functions, including the IT components that support these processes, and the recovery procedures needed in the case of a contingency or disaster. There is a designated COOP Coordinator named within the finalized COOP; the COOP document will be updated to designate one person with responsibility for COOP activation.

CNCS Privacy Response:

CNCS has made progress in implementing measures to protect privacy data as preliminary steps to assist in establishing conditions necessary to address the prior year weaknesses. These steps include hiring a new CISO and a Security Analyst, both in June 2015, and hiring a contractor (VMD System Integrators) in May 2015 to support the development of the Corporation's Cybersecurity Program. Additionally, CNCS developed a Privacy Controls Implementation Plan to document the organizational controls for protecting privacy and PII within the Corporation's systems." In addition, a Chief Privacy Officer (CPO) was in place in September 2015, and an initial version of Appendix J, to address NIST SP 800-53 Revision 4 privacy controls, was completed and signed July 28, 2015.

APPENDIX D: KEARNEY'S AND OIG'S COMMENTS ON PLANNED ACTIONS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") would like to thank the Corporation for National and Community Service (the Corporation) for the cooperation lent to us during the Federal Information Security Modernization Act of 2014 (FISMA) evaluation process and the comments provided to the draft fiscal year (FY) 2015 FISMA evaluation report. Many of the differences cited by the Corporation and Kearney are the result of timing. Kearney conducted the majority of our FISMA fieldwork during the period of May 2015 through July 2015. The Corporation hired its Chief Information Security Officer (CISO) and Security Analyst in June 2015. With the hiring of the CISO, the Corporation began implementing notable corrective actions to address the FY 2014 FISMA findings and recommendations in August and September 2015. Many of the corrective actions cited by the Corporation were not subject to Kearney audit procedures, as they occurred after the completion of Kearney's testwork.

Under "CNCS Overall Observations," the Corporation commented that two significant deficiencies related to continuous monitoring and risk management should be reduced to control deficiencies based on the progress made during FY 2015. Although the Corporation made progress in addressing the weaknesses by beginning to document and explore enterprise risk management, we noted that the weaknesses in the Corporation's security planning and assessment process continue. The process lacks a structured approach in performing security control assessments, which continue to put the Corporation at significant risk. Additionally, most of the recommendations under continuous monitoring and risk management were not fully resolved at the end of the FY 2015 evaluation period.

Kearney looks forward to working with the Corporation in FY 2016 to continue efforts to improve the Corporation's Information Security Program and completely implement the remaining open recommendations.

APPENDIX E: RESPONSES TO *DHS'S FY 2015 IG FISMA REPORTING METRICS*

1. **Continuous Monitoring Management**
   - **1.1. Utilizing the Information Security Continuous Monitoring (ISCM) maturity model definitions, in conjunction with the attributes outlined in Appendix A, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.**

     ISCM Maturity Model Results:
     People – Level 1 (Initial/Ad-hoc)
     Processes – Level 1 (Initial/Ad-hoc)
     Technology – Level 1 (Initial/Ad-hoc)
     Overall Maturity – Level 1 (Initial/Ad-hoc)
   - **1.2. Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.**

     Comments: The Corporation for National and Community Service (the Corporation) has not documented and fully implemented its ISCM Program. Key weaknesses include a lack of performance metrics advocated by the National Institute of Standards and Technology (NIST), such as the number of open and closed Plans of Action and Milestones (POA&M), overdue POA&Ms, security patches deployed within the Corporation's established timeframes, or an aging analysis (e.g., under 30 days, 30-60 days, over 60 days, etc.) of critical and high-risk security weaknesses from the Corporation's vulnerability scanner. In response to Kearney and Company's, P.C. (Kearney) observations, the Corporation indicated that it was developing an ISCM strategy and establishing performance metrics with its Managed Information Technology Services (MITS) contractor.
2. **Configuration Management**
   - **2.1. Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

     No. Comments: The Corporation has a documented process to implement configuration management for its desktops and servers. The configuration management process includes completing Security Impact Analyses (SIAs) for proposed changes prior to approval of such changes by the Technical Review Board and Production Change Control Board. However, the Corporation has not performed scans for configuration errors and deviations from the United States Government Configuration Baseline (USGCB) on its desktops and laptops or its standard configuration for Windows servers. In addition, the Corporation had not established performance metrics to measure the timeliness of patch remediation or ensured that vulnerabilities identified during system

vulnerability scans are remediated in a timely manner. These weaknesses indicate that the overall program is not consistent with FISMA requirements, Office of Management and Budget (OMB) policy, and applicable NIST guidelines.

2.1.1. Documented policies and procedures for configuration management.

Yes. Comments: The Corporation has published policies and procedures for configuration management.

2.1.2. Defined standard baseline configurations.

Yes. Comments: The Corporation has established a non-USGCB standard configuration baseline for its desktops.

2.1.3. Assessments of compliance with baseline configurations.

No. Comments: The Corporation has a configuration management process that describes the process to establish baseline configurations; however, the Corporation did not provide evidence to support that it periodically assesses compliance with USGCB settings for desktops or standard configurations for servers. According to the Corporation, technical difficulties with its vulnerability scanner prevent such configuration scans. The Corporation indicated its intent to replace its vulnerability scanner in FY 2016 and perform baseline configuration scans.

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

No. Comments: The Corporation has not developed and implemented a process to track the timeliness of security patch deployments based on the risk rating (i.e., critical, high, moderate, low) of identified vulnerabilities. The Corporation indicated that their MITS contractor alerts the Corporation to new vulnerabilities in weekly operational meetings.

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

No. Comments: The Corporation could not demonstrate its implementation of USGCB settings or document where the Corporation approved deviations from USGCB settings to accommodate deployed corporate applications. In response, the Corporation indicated that when changes to the desktop configuration are necessary, the Production Change Control Board (PCCB) reviews and approves such change requests. These approvals are recorded in meeting minutes.

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

Yes. Comments: The Corporation follows a policy and procedures to make changes to baseline configurations.

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

No Comments: The Corporation has software scanning capabilities; however, the tool utilized from October 2014 to July 2015 could not report configuration deviations and was not fully effective at identifying common application vulnerabilities in Adobe Reader, Adobe Flash, and Oracle Java. In response to the above observation, the Corporation indicated it would deploy Tenable Security Center (Nessus Pro).

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

No. Comments: The Corporation failed to remediate critical and high-severity level vulnerabilities in a timely manner.

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

No. Comments: The Corporation has established a patch management process; however, it was not effective as numerous critical and high-severity patches were not applied in a timely manner. The Corporation attributed the large number of critical and high-severity vulnerabilities to a flawed decommissioning process that allowed servers, scheduled for decommissioning, to remain powered on, but unmanaged.

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

Comments: While the Corporation has a vulnerability scanning tool, it did not utilize the tool to identify configuration deviations and did not leverage the vulnerability scanner to age unmitigated vulnerabilities by risk rating (i.e., critical, high, moderate, or low) or by months outstanding.

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

No. Comments: The Corporation has a deviation handling process but did not consistently follow its policy and document deviations.

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

No. Comments: The Corporation has a policy in place for mitigating risk associated with deviations. However, the Corporation did not have a process that included the scanning for configuration deviations from its baseline configuration. As such, a process for identifying, tracking, and accepting the risk of configuration deviations did not exist. In response to this observation, the Corporation indicated its intent to replace its vulnerability scanner and improve the oversight of it MITS contractor.

3. Identity and Access Management

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

Yes. Comments: Due to its legal status as a Federal corporation, the Corporation is not required by OMB to implement Personal Identity Verification (PIV). The Corporation has voluntarily implemented PIV for physical access and plans to implement PIV for logical access in fiscal year (FY) 2017.

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

Yes. Comments: The Corporation has documented policies and procedures for account and identity management.

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

Yes. Comments: The Corporation identifies all users, including Federal employees, contractors, and others, who access the Corporation's systems.

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

Yes. Comments: The Corporation has not implemented PIV for logical access because it is not required, but it is planning to do so in FY 2017.

3.1.4. Organization has 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. Comments: The Corporation's Government employees utilize PIV cards for physical access to the Corporation's Washington, D.C. headquarters, but not at state or regional offices or the five National Civilian Community Corps (NCCC) campus locations.

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

Yes. Comments: While users are not granted excessive access and user access is commensurate to user roles, the Corporation has further opportunities for improvement to ensure the timely removal of accounts belonging to departed employees and contractors.

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

Yes. Comments: The Corporation maintains an inventory of all hardware assets and distinguishes between those with and without user accounts.

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

No. Comments: The Corporation's access control policy was not consistently followed and some user accounts were not deactivated and deleted in a timely manner. In response to the noted observation, the Corporation indicated that it has implemented a new Off-Boarding system to improve its access control procedures. In addition, the Corporation stated that it completed a 100 percent review of all user accounts and privileged user accounts in October 2015.

3.1.8. Identifies and controls use of shared accounts.

Yes. Comments: Shared accounts are identified and controlled.

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

Comments: The Corporation ensures that users are granted access based on business needs and the user's role. The Corporation stated that its status as a Government corporation exempts it from HSPD 12 and FIPS Publication (PUB) 201 requirements to implement PIV cards for logical access. The Corporation plans to implement voluntarily PIV cards for logical access in FY 2017.

4. Incident Response and Reporting

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

Yes. Comments: The Corporation has established an Incident Response and Reporting Program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

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

Yes. Comments: The Corporation has sufficiently documented policies and procedures for incident response and reporting.

4.1.2. Comprehensive analysis, validation, and documentation of incidents.

Yes. Comments: The Corporation analyzed, validated, and documented incidents detected or reported in an automated system.

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

Yes. Comments: The Corporation reported all US-CERT reportable incidents in a timely manner.

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

Yes. Comments: The Corporation reported stolen laptops to law enforcement.

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

Yes. Comments: The Corporation resolved all incidents detected and reported such events, as required, in a timely manner.

4.1.6. Is capable of correlating incidents.

No. Comments: The Corporation uses Cisco Security Monitoring, Analysis, and Response System (MARS) to provide security monitoring, log correlation, and retention. However, MARS only retains two months of data at a time; thus, the correlations may not have enough data to identify potential trends or related incidents. Recognizing these limitations, the Corporation plans to implement Splunk for security monitoring, log correlation, and audit log retention.

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

No. Comments: The Corporation uses MARS to provide security monitoring, log correlation, and audit log retention. The Corporation relied on an obsolete and unsupported vendor tool for network audit log aggregation and automatic alerting. In response to the noted observation, the Corporation indicated that it plans to transition to a new audit log correlation tool, Splunk, while continuing to use MARS as a network access control tool. Additionally, the Corporation stated that it receives periodic "cyber hygiene" reports from DHS that highlights fewer security vulnerabilities than other agencies.

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

Comments: The Corporation has adequate policies and procedures in place to perform incident response and reporting. Continued management attention is needed to upgrade the Corporation's network monitoring capabilities.

5. Risk Management

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

No. Comments: The Corporation has developed an risk management plan that describes the three tiers of management to cover the enterprise level (i.e., Tier 1), the missions/business level (i.e., Tier 2), and the information systems level (i.e., Tier 3); however, the plan is not fully implemented. Monthly IT Steering Committee meetings are held to make decisions concerning the information systems level. However, risks are not assessed at the different business tiers as part of regular information security assessments or other program- or financial-oriented risk assessments. For example, a Business Impact Analysis (BIA), a Tier 2 risk assessment activity, has not been conducted in FY 2015 to identify mission-critical business functions and quantify the

impact of a loss if a supporting information system (i.e., eGrants, eSPAN) was unavailable. In addition, the Information Assurance Plan (IAP), BIA, and Continuity of Operations Plan (COOP) need to be developed and/or updated to address risks in Tiers 1 and 2 and to involve the system owners in the risk management process.

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

No. Comments: The Corporation has not fully documented and implemented its risk management practices. There is a lack of integration between the business owners and the Office of Information Technology (OIT). Further, the Corporation is not compliant with the NIST SP 800-37, Revision (Rev.) 1 guideline to "ensure that risk-based decision making is integrated into every aspect of the organization."

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

No. Comments: The Corporation has not developed BIAs for major systems to determine business risks. The business owners have limited involvement, which undermines the Corporation's ability to address and mitigate risks associated with the operation and use of information systems that support its missions and business functions. In response to the noted observation, the Corporation indicated that it has developed a draft Enterprise Risk Management Plan that is awaiting signature by the Chief Executive Officer (CEO) and begun holding monthly Integrity Steering Committee meetings.

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

Yes. Comments: The Corporation has conducted risk assessments for major systems.

5.1.4. Has an up-to-date system inventory.

Yes. Comments: The Corporation system inventory is up-to-date.

5.1.5. Categorizes information systems in accordance with government policies.

Yes. Comments: The Corporation has completed FIPS PUB 199 system categorizations for its major information systems.

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

No. Comments: The Corporation selects baseline security controls and documents those controls in a System Security Plan (SSP). However, the Corporation does not have a common controls security plan to address the security controls that the Corporation must implement (i.e., Program Management security controls), as opposed to the security controls implemented by it MDCS contractor.

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

No. Comments: The Corporation has not consistently implemented its tailored security controls for individual information systems and has not defined its "organizational defined frequency" for operational controls, such as the daily / weekly / monthly audit log review.

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

No. Comments: The Corporation has conducted current security assessments; however, it has not utilized an independent security assessor, as required by NIST, for its moderate-impact systems. Further, the Corporation relies extensively on its IT vendors to perform security control assessments used to process the Corporation's information. The Corporation has not developed standard test cases to capture evidence of control effectiveness, promoted re-use of tailored test cases, or established a standard sampling plan to ensure consistency across security control assessments performed by different IT vendors. In response to the noted observation, the Corporation indicated its intent to task its information security contractor to assist in developing tailored test cases, a sampling plan, and supporting independent security assessments.

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

No. Comments: The Corporation does not currently look at risk from an organization-wide or mission/business process-wide risk assessment approach. Instead, the security assessment and authorization process focuses on Tier 3 (information system risks). In response to the noted observation, the Corporation stated that it has developed a draft Enterprise Risk Management Policy and begun holding monthly Integrity Steering Committee meetings.

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

No. Comments: The Corporation lacks a documented process to communicate risks within the Corporation to business owners and executive management. In response to the noted observation, the Corporation stated that it has developed a draft Enterprise Risk Management Policy and begun holding monthly Integrity Steering Committee meetings.

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

Yes. Comments: The Chief Information Officer (CIO) is briefed monthly on the progress of remediating POA&M items. The Chief Operating Officer (COO) is briefed quarterly on POA&M progress. In June 2015, the Corporation hired a Chief Information Security Officer (CISO) and Information Assurance Specialist to assist in the monthly information security briefings.

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

No. Comments: The Corporation's IAP does not contain responsibilities for all the stakeholders listed to participate actively in the management of information system security. In response to the noted observation, the Corporation stated that it updated and renamed the Information Assurance Policy to the CNCS Cybersecurity Policy and that this document is currently under review. According to the Corporation, this updated draft policy identifies the roles and responsibilities of information system owners and common control providers, CIO, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks.

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

Yes. Comments: The Corporation has current security authorization packages for all major systems. However, weaknesses exist in the completeness and accuracy of individual information system POA&Ms.

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

Yes. Comments: The Corporation has one major cloud system, which is hosted by a commercial provider that serves multiple Federal customers. The provider has FedRAMP approval.

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

Yes. Comments: The Corporation has a contract, including an SLA, in place with its FedRAMP-certified service provider.

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

Comments: The Corporation lacks a comprehensive risk management program, which encompasses the three tiers defined in NIST SP 800-39. Without such a program, an effective risk-based Information Security Program cannot be assured. The Corporation cannot systematically apply limited resources to the areas of greatest risk when those areas have not been identified. In response to the noted observation, the Corporation stated that it has developed a draft Enterprise Risk Management Policy and begun holding monthly Integrity Steering Committee meetings.

6. Security Training

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

No. Comments: The Corporation has not implemented a formal role-based Information Security Training Program for individuals with significant information security responsibilities. Annual user awareness training did not occur in the period of October 1, 2014 through September 30, 2015. In response to the noted weakness, the Corporation stated that it held annual end-user awareness training and formal role-based for employees with significant information security responsibilities during October 2015.

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

Yes. Comments: The Corporation has documented policies and procedures that include annual user security awareness.

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

Yes. Comments: The Corporation has documented policies and procedures that require specialized training for users with significant information security responsibilities. However, the Corporation has not implemented specialized training for users with significant information security responsibilities.

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

No. Comments: The Corporation has documented policies and procedures for security role-based training; however, the training is not employed for all users with significant information security responsibilities. In response to the noted weakness, the Corporation stated that it held annual end-user awareness training and formal role-based for employees with significant information security responsibilities during October 2015.

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.

Yes. Comments: The Corporation uses its learning management system to track security training awareness completion by all users.

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.

No. Comments: The Corporation does not employ appropriate tracking of completion for special users with significant information security responsibilities. In response to the noted weakness, the Corporation stated that it held privileged user training and formal role-based for employees with significant information security responsibilities during October 2015.

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

Yes. Comments: The Corporation training material content covers all relevant user security awareness topics for the organization.

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

Comments: The Corporation's current role-based training material consists of PowerPoint slides focused on promoting awareness of assigned responsibilities rather than training, which NIST defines as building knowledge and skills to facilitate job performance. In addition, the Corporation does not confirm that its contractors complete the required security training. In response to the noted weakness, the Corporation indicated that the privileged user and role-based training would be revised annually; privileged users will sign the Privileged Users and System Administrator Rules of Behavior (RoB) Agreement annually. Similarly, users with significant information security responsibilities will complete role-based training annually. In addition, all IT users must complete the CNCS Cybersecurity User Training, which includes topics on privacy, phishing, and PII, and submit signed RoB annually.

7. Plan Of Action & Milestones (POA&M)

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

No. Comments: In FY 2015, the Corporation developed new standard operating procedures for completing POA&M items and created a corporate-level POA&M to address information security weaknesses at

the enterprise level. However, the Corporation's POA&M program has not been effectively implemented, as evidenced by the omission of critical information (i.e. scheduled completion dates, responsible party, and resources required to remediate weaknesses) in many of the POA&M items across its 11 individual POA&M tracking spreadsheets.

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

Yes. Comments: The Corporation has documented policy and procedures in the Corporation's IAP and POA&M Guidelines documents.

7.1.2. Tracks, prioritizes, and remediates weaknesses.

No. Comments: The Corporation includes most weaknesses in the POA&M; however, the Corporation does not have an adequate POA&M management process in place to ensure all known security weaknesses are recorded. For example, items omitted from the Corporation's information system POA&Ms include high-risk, technical vulnerabilities from monthly vulnerability scans that were outstanding over 30 days and could not be remediated within this timeframe. In response to the noted observation, the Corporation indicated that it is separately tracking and reporting technical vulnerabilities in weekly and monthly reports.

7.1.3. Ensures remediation plans are effective for correcting weaknesses.

Yes. Comments: The Corporation POA&M has corrective action plans for most weaknesses.

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

No. Comments: The Corporation did not consistently review its POA&Ms and update POA&M items when milestone due dates were missed. Further, POA&Ms frequently did not contain explanations for why initial POA&M milestone dates were missed.

7.1.5. Ensures resources and ownership are provided for correcting weaknesses.

No. Comments: The Corporation's POA&Ms for individual information systems identify ownership for individual weaknesses; however, these POA&Ms generally do not identify resource requirements. Further, many POA&M items did not identify the resources (man-hours and/or costs) required to resolve open tasks and update milestone completion dates when due dates were missed. In response to the noted weakness, the Corporation stated that its IT contracts are generally firm-fixed price contracts and resolution of the noted weakness generally remains with the contractor. As such, the resources required field is left blank.

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).

No. Comments: While the Corporation has developed new operating procedures for POA&M management, these procedures have not been consistently implemented. The POA&Ms for the Corporation's 11 information systems do not contain all weaknesses identified during security control assessments. Weaknesses omitted from the POA&Ms include high-risk, technical vulnerabilities from monthly vulnerability scans that were outstanding over 30 days.

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

No. Comments: The Corporation's POA&Ms, including its Corporate-level POA&M, generally did not include any resource requirements or associated costs. In response to the noted weakness, the Corporation indicated that its IT contracts are generally firm-fixed price and the contractor is responsible for the remediation costs.

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:CA5; OMB M-04-25).

Yes. Comments: The CIO is provided with an overall POA&M status on a regular basis and conducts quarterly review of POA&M activities.

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

Comments: The Corporation has documented a POA&M Program that has the potential to be an effective tool in remediating identified weaknesses. However, the Corporation has not fully implemented its procedures. As a result, weaknesses are not remediated in a timely manner and resource requirements for remediation cannot be readily identified. With the appointments of the new CISO and Security Analyst, the Corporation should have the resources to resolve the POA&M findings and recommendations.

8. Remote Access Management

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

No. Comments: The Corporation does not have a remote access policy. The Corporation rescinded the previous remote access policy in 2015 and is drafting a new policy.

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).

No. Comments: The Corporation does not have a remote access policy. The Corporation rescinded the previous policy in 2015 and is drafting a new policy.

8.1.2. Protects against unauthorized connections or subversion of authorized connections.

Yes. Comments: The Corporation uses two primary remote access types. Government-issued equipment uses "Always-on" Virtual Private Network (VPN) access and non-Government-furnished equipment uses the web-based remote access portal, Web VPN Portal. Corporation users of non-Government-furnished equipment are required to provide unique identifiers (e.g., username, pin/token code, and passcode) for access. Government-furnished equipment automatically authenticates to the Corporation's network based on a digital certificate and provides complete remote access without the need for additional credentials.

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

Yes. Comments: The Corporation employs user IDs and hardware tokens to uniquely identify and authenticate users.

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

Yes. Comments: The Corporation has a developed remote telework policy.

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

Yes. Comments: The Corporation users of non-Government-furnished equipment are required to provide unique identifiers (e.g., username, pin/token code, and passcode) for access. Government-furnished equipment automatically opens a connection to the Corporation network and provides complete remote access without the need for additional credentials.

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

No. Comments: All Corporation remote access connections over public networks are not encrypted with FIPS PUB 140-2-approved methods. For example, the Corporation was not operating the current version of the Cisco VPN software for its VPN network device and was using unapproved protocols (i.e., TLS 1.0) and cryptographic algorithms (SHA-1). In response to the noted weakness, the Corporation stated that its current hardware is unable to support TLS 1.2 due to firmware limitations and its contractor plans to upgrade the current hardware by March 2016.

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

Yes. Comments: The Corporation has implemented a time-out of 30 minutes for remote access connections.

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

Yes. Comments: The Corporation disables lost or stolen devices and reports the loss to US-CERT in a timely manner.

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

Yes. Comments: The Corporation provided a draft Rules of Behavior (RoB) that includes a system access restriction policy. The new policy requires users to connect to Corporation systems only through approved methods, such as via Government-furnished equipment. Subsequently, the Corporation implemented the new RoB on September 30, 2015.

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

Yes. Comments: During the FISMA evaluation, the Corporation provided a draft RoB for remote access and subsequently implemented the new RoB on September 30, 2015.

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

Comments: The Corporation's VPN device used for remote access only supports TLS 1.0. NIST SP 800-52, Rev. 1, Section 3, *Minimum Requirements for TLS Servers*, subsection 3.1, *Protocol Version Support*, states, "TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended." The Corporation's oversight of the VPN solution, managed by its contractor, did not identify the use of non-approved FIPS PUB 140-2 protocols or that the Corporation's deployed VPN connection device supported only TLS 1.0. In response to the noted weakness, the Corporation stated its intent to replace its VPN hardware to support approved FIPS 140-2 protocols and approved cryptographic algorithms.

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

Yes. Comments: The Corporation has a policy, its RoB, against connecting personal devices to the Corporation's network via VPN technology. However, its ability to detect and block rogue devices is limited, as the Corporation's VPN appliance authenticates remote devices using a shared digital certificate rather than a digital certificate that is unique to every device.

9. Contingency Planning

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

No. Comments: The Corporation lacked current system-specific contingency plans for the major systems and did not test the Disaster Recovery Plan or system contingency plans for Corporation-hosted systems in FY 2015. In addition, the Corporation has not updated its BIAs for its major applications; therefore, the program is not consistent

with FISMA requirements, OMB policy, and applicable NIST guidelines. In response to the noted weakness, the Corporation indicated its intent to prepare an enterprise-wide COOP and participate in annual government-wide disaster recover exercises. As part of its readiness efforts, the Corporation will designate a COOP coordinator and ensure its MITS contractor prepares a BIA and DRP for the Corporation's LAN/WAN infrastructure.

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).

No. Comments: The Corporation has developed a draft COOP to reduce the impact of a disruptive event or disaster. However, the Corporation did not update the COOP and IT DRP to reflect the migration to Microsoft Office 365 and One Drive in its COOP. Further, the COOP has not been tested. In response to the noted weakness, the Corporation indicated its intent to remediate the weakness by finalizing the COOP, designating a COOP coordinator, and ensuring its MITS contractor prepares a BIA and DRP for the Corporation's LAN/WAN infrastructure.

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

No. Comments: The Corporation has not created BIAs for its major systems (i.e., eSPAN, Momentum, and eGrants) and incorporated the results in the IT DRP. In response to the noted weaknesses, the Corporation stated that it is identifying the stakeholders for mission/business functions to complete the BIA and update the COOP and DRP. This effort will also facilitate the identification of mission-essential functions, including the IT components that support these processes, and the recovery procedures needed in the case of a contingency or disaster.

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

No. Comments: While the Corporation has an overall COOP, the Corporation does not have an IT DRP. In addition, major information systems were lacking a contingency plan. While these weaknesses exist, some of the Corporation's five NCCC campuses developed emergency response plans. In response to the noted weaknesses, the Corporation stated that it is identifying the stakeholders for mission/business functions to complete the BIA and update the COOP and DRP. This effort will also facilitate the identification of mission-essential functions, including the IT components that support these

processes, and the recovery procedures needed in the case of a contingency or disaster.

9.1.4. Testing of system-specific contingency plans.

No. Comments: The Corporation did not conduct contingency plan tests for any of the Corporation-hosted major systems (eSPAN, Momentum, nor eGrants) in FY 2015.

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

No. Comments: The Corporation has a documented enterprise Business Continuity Plan and DRP; however, the Corporation has not updated its BIA to identify organizational risks that should be addressed in the COOP, nor developed an agency-wide COOP, a GSS DRP, and a financial system Contingency Plan. In response to the noted weakness, the Corporation indicated its intent to remediate the weakness by finalizing the COOP, designating a COOP coordinator, and ensuring its MITS contractor prepares a BIA and DRP for the Corporation's LAN/WAN infrastructure.

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

No. Comments: The Corporation does not have current TT&E programs for contingency plans.

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

No. Comments: The Corporation did not test or exercise the IT DRP in FY 2015 for any of its key systems.

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

No. Comments: The Corporation did not produce any after-action reports for Corporation-hosted systems since it did not hold any exercises in FY 2015.

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

Yes. Comments: The Corporation maintains an alternate processing site located a sufficient distance from the primary processing site. All contingency plans identify this site.

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

Yes. Comments: The Corporation conducted regular backups.

9.1.11. Contingency planning that considers supply chain threats.

No. Comments: The Corporation COOP and IT DRP did not contain information regarding essential business suppliers. The Corporation relies heavily on its information system vendors and did not establish emergency agreements to ship critical laptops and other necessary

office equipment to its disaster recovery site. In response to the noted weakness, CNCS utilizes Trade Agreement Acts (TAA) approved vendors to mitigate supply chain threats when available.

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

Comments: The Corporation has an alternate processing site for its data center; however, it did not test its ability to recover key servers and key information systems (e.g., eGrants, eSPAN, MyAmeriCorps Portal) at the alternate site. In addition, the Corporation's disaster recovery documentation does not demonstrate consideration of all of the Corporation's essential functions and missions. The Corporation's BIA specifically states that it is not meant to address all essential business functions. The Corporation's DRP is written specifically for the GSS and is not representative of the Corporation as a whole, including other key IT contractors and systems to include its major systems (eSPAN, eGrants, and Momentum).

10. Contractor Systems

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

No. Comments: The Corporation has not established and implemented policies and procedures sufficient for effective oversight of multiple contractor systems. Additionally, the Corporation has not developed meaningful and reportable performance metrics to evaluate the IT contractors' performance and incorporated such performance metrics into its IT contracts. In response to the noted weaknesses, the Corporation stated that it plans to leverage its information assurance support contractor to provide additional, independent oversight of the Corporation's IT contractors.

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

No. Comments: Although the Corporation IAP requires the security oversight of contractor systems, the Corporation has not developed policies and procedures to do so.

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

No. Comments: The Corporation received an insufficient amount of detail and evaluation criteria necessary for review of security assessment documentation and security performance measures required from its IT contractors.

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

Yes. Comments: The Corporation maintains a systems inventory that identifies contractor systems and the service provider for those systems.

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

Yes. Comments: The Corporation system inventory includes the required system interface information.

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.

Yes. Comments: The Corporation has appropriate agreements for all contractor systems.

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

Yes. Comments: Inventory of contractor systems is maintained. Information in the inventory is complete.

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

Comments: Kearney reviewed the Corporation's list of service providers and noted that the "Criteria used for tracking contract performance" column was blank. The document lists other contractor information (e.g., contract number, contract type, and type of service), but does not provide any information about how the Corporation plans on implementing contractor oversight or evaluate performance metrics. In addition, the Corporation does not include SLAs within existing IT contracts to ensure contractors are aware of the performance metrics they must meet.

APPENDIX F: RESULTS FROM FIELD OFFICE ASSESSMENTS

The Corporation for National and Community Service (the Corporation) has five National Civilian Community Corps (NCCC) campuses, one Volunteers in Service to American (VISTA) Member Support Unit (VMSU), and many state offices in cities throughout the United States. In support of the Federal Information Security Modernization Act of 2014 (FISMA) evaluation of the Corporation, Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") conducted four site visits. We conducted field office assessments at the Pennsylvania State Office and the Field Financial Management Center (FFMC) in Philadelphia on July 30, 2015; and at the Maryland State Office and NCCC Atlantic Region campus (Baltimore) the following day on July 31, 2015. As part of our assessment strategy, we performed walkthroughs of workspace and office suite areas to identify unsecured personally identifiable information (PII) exposures. Kearney's visits to these locations also included an evaluation of controls to ensure acceptable usage of Corporation network resources, physical security, rogue connections, PII management, and a search for inappropriate material on Corporation workstations.

At each location, Kearney toured the facilities and noted the physical locations for storage of PII (paper and portable electronic). Kearney noted that all locations stored PII records in locked file cabinets within locked rooms. However, Kearney noted that PII was maintained beyond the retention period.[60] We also noted deficiencies in physical access controls at the field offices. These observations were communicated to Corporation management at both the field locations and at Headquarters. Kearney did not detect any unapproved wireless access points within proximity of the field offices. We noted that the Managed Information Technology Services (MITS) contractor-deployed technology to manage the configuration of the Corporation's laptops and deploy security patches.

[60] Disposal of PII should be conducted in accordance with the retention schedules approved by the National Archives and Records Administration (NARA), as well as in accordance with agency litigation holds.

APPENDIX G: ABBREVIATIONS AND ACRONYMS

Acronym	Definition
AD	Active Directory
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BPA	Blanket Purchase Agreement
BYOD	Bring-Your-Own-Device
CD	Control Deficiency
CDM	Continuous Diagnostics and Mitigation
CEO	Chief Executive Officer
CET	Continuity of Operations Plan Executive Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CNCS/Corporatio	Corporation for National and Community Service
CO	Contracting Officer
COO	Chief Operating Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer's Representative
COS	Contractor On-boarding System
COTS	Commercial-off-the-Shelf
CPARS	Contractor Performance Assessment Reporting System
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
CS&C	Cybersecurity and Communications
CSP	Cloud Service Provider
DHS	Department of Homeland Security
DOS	Denial-of-Service
DRP	Disaster Recovery Plan
EAP	Enterprise Architecture Plan
EOL	End-of-Life
EOS	Employee On-boarding System
eSPAN	Electronic System for Programs Agreements and National Service
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FFMC	Field Financial Management Center
FIPS	Federal Information Processing Standards

Acronym	Definition
FISMA of 2002	Federal Information Security Management Act of 2002
FISMA of 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IAM	Identity and Access Management
IAPS	Information Assurance Program Support
IG	Inspector General
IP	Internet Protocol
ISCM	Information Security Continuous Monitoring
ISO	Information Security Owner
ISSM	Information System Security Managers
ISSO	Information System Security Officer
IT	Information Technology
ITIL	IT Infrastructure Library
GAO	Government Accountability Office
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
Kearney	Kearney & Company, P.C.
LAN	Local Area Network
MA	Major Applications
MARS	CISCO Security – Monitoring, Analysis, and Response System
MDCS	Managed Data Center Services
MITS	Managed Information Technology Services
MOA	Memorandum of Agreement
Momentum	Momentum Financial Management System
MPLS	Multiprotocol Label Switching
NARA	National Archives and Records Administration
NCCC	National Civilian Community Corps
NFR	Notification of Finding and Recommendation
OEM	Operations, Engineering and Maintenance
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OPS	Office of Procurement Services
NIST	National Institute of Standards and Technology
PHI	Protected Health Information

Acronym	Definition
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
POA&M	Plan of Actions & Milestones
PRA	Paperwork Reduction Act of 1995
PUB	Publication
Rev.	Revision
RoB	Rules of Behavior
RMF	Risk Management Framework
SA	System Administrators
SA&A	Security Assessment and Authorization
SAR	Security Authorization Report
SCAP	Security Content Automation Protocol
SD	Significant Deficiency
SDLC	System Development Lifecycle
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SoD	Segregation of Duties
SOP	Standard Operating Procedures
SOW	Statement of Work
SP	Special Publication
SSL	Secure Socket Layer
SSP	System Security Plan
TB	Terabyte
TLS	Transport Layer Security
TRUST	National Service Trust
TT&E	Test, Training, & Exercise
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USB	Universal Serial Bus
USGCB	United States Government Compliance Baseline
USPS	United States Postal Service
VISTA	Volunteers In Service To America
VLAN	Virtual Local Area Network
VMSU	Volunteers in Service to American Member Support Unit

Acronym	Definition
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX H: REFERENCED DOCUMENTS

Federal Law:

- Federal Information Modernization Act of 2014 (FISMA)
- Federal Information Security Management Act of 2002 (FISMA) (Title III, Public Law [P.L.] No. 107-347)
- Privacy Act of 1974 (P.L. No. 93-579)
- e-Government Act of 2002 (P.L. No. 107-347)
- Clinger-Cohen Act of 1996 (CCA)
- Paperwork Reduction Act of 1980.

Office of Management and Budget (OMB):

- Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- Circular A-123, *Management's Responsibility for Internal Control, Section II*
- Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Actions and Milestones*
- Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- Memorandum M-06-16, *Protection of Sensitive Agency Information*
- Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
- OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*.

Federal Information Processing Standards (FIPS) Publications (PUB):

- *202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*,
- 199, *Standards for Security Categorization of Federal Information and Information Systems*
- 140-2, *Security Requirements for Cryptographic Modules.*

United States Computer Emergency Readiness Team (US-CERT):

- Federal Incident Reporting Guidelines, *Federal Agency Incident Categories.*

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

- 800-16, Inform*ation Technology Security Training Requirements: A Role- and Performance-Based Model*
- 800-18, Revision (Rev.) 1, *Guide for Developing Security Plans for Federal*

Information 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*
- 800-39, *Managing Information Security Risk*
- 800-52, Rev. 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
- 800-55, *Performance Measurement Guide for Information Security*
- 800-58, *Security Considerations for Voice Over IP Systems*
- 800-61, *Revision 2, Computer Security Incident Handling Guide*
- 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
- 800-92, *Guide to Computer Security Log Management*
- 800-111, *Guide to Storage Encryption Technologies*
- 800-113, *Guide to SSL VPNs*
- 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organization.*

Additional Information and Copies

To report alleged fraud, waste, abuse, mismanagement, or any other kind of criminal or non-criminal misconduct relative to the Corporation for National and Community Service (the Corporation) programs or operations:

Corporation for National and Community Service
Office of Inspector General
Phone: 1-800-452-8210
Fax: 202-606-9397
Website: http://www.cncsoig.gov/hotline

For the deaf or hard of hearing, dial Federal Relay Service (FRS) at 800-877-8339 and give the hotline number to the relay operator.

Additional copies of this report can be obtained by contacting the Corporation's Office of Inspector General (OIG) at:

Corporation for National and Community Service
Office of Inspector General
1201 New York Ave, NW, Suite 830
Washington, D.C. 20525
(202) 606-9390