Office of Inspector General
Corporation for National and Community Service

FISCAL YEAR 2016
FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT 17-03

Prepared by:

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

This report was issued to Corporation management on December 22, 2016. Under the laws and regulations governing audit follow up, the Corporation is to make final management decisions on the report's findings and recommendations no later than June 22, 2017, and complete its corrective actions by December 22, 2017. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Office of Inspector General
Corporation for
NATIONAL & COMMUNITY SERVICE

December 22, 2016

TO: Wendy Spencer
Chief Executive Officer

FROM: Kenneth Bach /s/
Deputy Inspector General

SUBJECT: Fiscal Year 2016 Federal Information Security Modernization Act (FISMA)
Evaluation of the Corporation for National and Community Service
(OIG Report 17-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 17-03, *Fiscal Year 2016 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).

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 202-606-9377.

Attachment

cc: Jeffrey Page, Chief Operating Officer and Chief Financial Officer
Tom Hanley, Chief Information Officer
Andrea Simpson, Chief Information Security Officer
Lori Giblin, Chief Risk Officer
Jeremy Joseph, General Counsel
Tyler Harding, Engagement Principal, Kearney & Company, P.C.

Fiscal Year 2016 Federal Information Security Modernization Act Evaluation for the

Corporation for National and Community Service

December 21 2016

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. Under contract with the Office of Inspector General (OIG), Kearney performed the FY 2016 FISMA evaluation at CNCS. Its 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, as well as to evaluate the operating effectiveness of the information security and privacy controls over those systems.

Recommendations
Despite significant progress in addressing recommendations from prior FISMA evaluations, additional work is needed to address shortfalls in effective IT security controls.

CNCS should continue efforts to mature its ISCM Program, implement its Information Security Risk Management Program, and establish performance metrics to achieve adequate security.

December 2016

Despite Progress, Weaknesses Persist in Information Security and Privacy at CNCS

Office of Inspector General
Corporation for NATIONAL & COMMUNITY SERVICE

What OIG Found
The Corporation for National and Community Service (the Corporation or CNCS) has made significant progress in addressing the information security and privacy weaknesses identified in last year's Federal Information Security Modernization Act of 2014 (FISMA) evaluation, resolving eight of 17 findings from FY 2015 and closing 67 of 90 recommendations open from prior years. CNCS has improved and updated its policies and procedures for key security program areas, *e.g.*, information security continuous monitoring (ISCM), risk management and Plan of Action and Milestones (POA&M) management. It has also entered into new service level agreements with the information technology (IT) contractor that manages the Corporation's desktops, servers and network infrastructure. These improvements led Kearney & Company, P.C. (Kearney) to reduce the severity of two previous program weaknesses from Significant Deficiencies to Control Deficiencies. Evaluators determined that the Corporation implemented improvements to close all seven recommendations related to privacy controls for protection of personally identifiable information (PII).

Nevertheless, much work remains to make information security fully effective at CNCS. The FY 2016 FISMA evaluation uncovered two new weaknesses relating to: (1) secure configuration management policies, procedures and practices; and (2) monitoring and remediation of server backup failures. CNCS's ISCM and Incident Response Program are rated at Level 2: *Defined* on a maturity scale that ranges from Level 1: *Ad hoc* to Level 5: *Optimized*. Of the 57 security metrics in the remaining areas, testing identified 25 instances of noncompliance with applicable laws, regulations and authoritative guidance governing information security.

FY 2016 FISMA Evaluation Results

NIST Cybersecurity Framework Function	FY 2016 IG FISMA Metric	# of DHS Exceptions / Total DHS IG Questions	Security Control Effectiveness
Identify	1.1 Risk Management	2 of 16	Control Deficiency
	1.2 Contractor Systems	2 of 3	Control Deficiency
Protect	2.1 Configuration Management	6 of 9	Control Deficiency
	2.2 Identity and Access Management	8 of 14	Control Deficiency
	2.3 Security and Privacy Training	2 of 5	Demonstrates Effectiveness
Detect	3.1 Information Security Continuous Monitoring	People, Processes, and Technology Assessed at Level 2: Defined	Control Deficiency
Respond	4.1 Incident Response	People, Processes, and Technology Assessed at Level 2: Defined	Control Deficiency
Recover	5.1 Contingency Planning	5 of 10	Control Deficiency
N/A	†Privacy	N/A	Demonstrates Effectiveness

† - Consistent with the addition of privacy controls to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, OIG contracted with Kearney to evaluate the Corporation's implementation of privacy controls as part of the FY 2016 FISMA evaluation.

TABLE OF CONTENTS

Page #

1. COVER LETTER

December 21, 2016

Ms. Wendy Spencer
Chief Executive Officer
Corporation for National and Community Service
250 E Street, SW, 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" or "CNCS") 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) 2016 FISMA evaluation of the Corporation's information technology (IT) policies, procedures, and practices. We are pleased to provide this FY 2016 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 *FY 2016 Inspector General (IG) Federal Information Security Modernization Act of 2014 Reporting Metrics v1.1.3*, dated September 26, 2016 (referred to as the *DHS FY 2016 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's methodology for the FY 2016 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], Momentum Financial Management System [Momentum]), and VISTA Healthcare Benefits [VHB][1] 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 met the *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency (CIGIE),[2] and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

Since the FY 2015 FISMA evaluation, the Corporation has taken steps to improve its overall Information Security and Privacy Program and its compliance with the FISMA legislation, OMB guidance, and applicable NIST SPs. The Corporation closed eight of 17 findings from the FY 2015 FISMA evaluation (i.e., Organizational Conflict of Interest) and closed 67 of 90[3] open recommendations from the FY 2014 and FY 2015 FISMA evaluations. Further, the Corporation has developed and documented an IT Strategic Plan and Enterprise Architecture Plan, created and delivered role-based training for employees with key security responsibilities, and implemented service level agreements (SLA) on it largest IT contract.

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 September 30, 2016, we concluded that the Corporation's Information Security and Privacy Program were not fully compliant with respect to FISMA legislation, OMB guidance, and applicable NIST SPs. In addition to the eight[4] FISMA metric domains, we evaluated privacy controls as a separate area, for a total of nine areas reviewed. Our testing found the controls need improvement in seven of the nine areas examined.

Annually, OMB and DHS provide specific instructions and request OIGs to prepare responses to specific information security metric questions. Based on the *DHS FY 2016 IG FISMA Reporting Metrics*, a FISMA evaluation addresses eight specific aspects of information security, subdivided

[1] VISTA Healthcare Benefits is a major application managed by International Medical Group, Inc. (IMG). Referred to as DIALX by IMG, VISTA Healthcare Benefits is composed of a group of systems used to provide administrative, medical management, document imaging, and claims processing for members participating in the Corporation's VISTA program.

[2] 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.

[3] In addition to the 90 prior-year recommendations, Kearney added five recommendations to FY 2014 NFR #2. Please see Appendix B: *Status of Prior Year Findings* for a complete list.

[4] Key FISMA metrics identified in the *FY 2016 DHS IG FISMA Metrics* comprise: Risk Management, Contractor Systems, Configuration Management, Identity and Access Management (IAM), Security and Privacy Training, Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning.

into 57 individual security metrics. **Of the 57 security metrics in the six domains without a maturity model, our testing identified 25 instances of noncompliance with OMB guidance and NIST SPs. We grouped these instances of noncompliance into 11 findings (two new findings in FY 2016 and nine repeated findings from prior years).** For the two domains with maturity models, Kearney rated the Corporation's Information Security Continuous Monitoring (ISCM) Program and Incident Response (IR) Program maturity at a Level 2: *Defined* for both domains. Of the nine repeated findings, there are seven open findings from FY 2014 and two findings from FY 2015. Since the FY 2015 FISMA report, the Corporation addressed 67 recommendations, while 23 recommendations from prior years remain open. Appendix B Resolution Status of FY 2013, 2014, 2015 NFRs provides details on the status of remediation. This report includes 13 new recommendations to strengthen the Corporation's Information Security Program. Five of the 13 new recommendations address new weaknesses identified with the Corporation's vulnerability scanning and remediation practices.

Kearney recognizes that the Corporation is operating in an environment of constrained personnel resources and limited funding due to an effort to modernize[5] its IT infrastructure and grant application. Nevertheless, continued management attention is necessary to resolve the long-standing IT security 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 due to changes in conditions, the deterioration of compliance with controls, or the introduction of new risk.

We have included detailed information in a series of appendices. Appendix A: FY 2016 New Finding provides the full text of each new FISMA finding. Appendix B: Status of Prior-Year Findings provides the status of findings and recommendations from prior years. Appendix C: Management Response provides the Corporation's response to the draft FISMA report. Appendix D: 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

Kearney & Company, P.C.
December 21, 2016

[5] OIT's goal for IT modernization 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.

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 660 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 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 a FISMA inventory of seven information systems – the Network (GSS), eSPAN, Momentum, VISTA Health Benefits, AmeriCorps Childcare Benefits System, NCCC Health Benefits, and Public Websites. The Federal Information Processing Standard (FIPS) Publication (PUB) 199[6] security categorization levels of these systems are moderate (six of seven systems) and low (one system). Of the seven information systems, five are hosted and operated by third-party service providers. The Corporation's network consists of multiple sites: Headquarters (HQ), 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 commercially managed high-speed network connections.

Sustaining high levels of service at cost effective rates 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 five of its seven information systems, it retains responsibility, by law, for complying with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) and security control implementation.

[6] 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 share responsibility for managing 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 on July 30, 2015 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 and central database for maintaining the Corporation's application and grant data and AmeriCorps program and member data, including member related payments. eSPAN tracks AmeriCorps members and TRUST educational awards, including awards made to all individuals in the 23-year history of the Corporation (approximately 1.25 million individuals)
3. **Momentum Financial Management System (Momentum) –** Multi-tiered, 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 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 or Act) was enacted into United States Federal law as P.L. 113-283 (December 18, 2014), 44 U.S.C. §§ 3551-58. The 2014 Act 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, further references to FISMA in this report refer to the 2014 legislation.

FISMA was updated 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, as directed by OMB, but no later than November 10 of each year.

While the 2014 Act 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.[7]

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

1. 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
2. Compliance with information security policies, procedures, standards, and guidelines issued by OMB and DHS under the authority of FISMA
3. 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
4. Annual security awareness training programs
5. 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

[7] § 3555 *Annual Independent Evaluation,* Federal Information Security Modernization Act of 2014.

6. Periodic risk assessments
7. Processes to manage remedial actions for addressing deficiencies
8. Procedures for detecting, reporting, and responding to security incidents
9. Plans and procedures to ensure continuity of operations for information systems
10. Annual reporting on the adequacy and effectiveness of the Information Security Program to OMB, the Secretary of Homeland Security, and Congress.

OMB is responsible for reporting a summary of the results of an agency's compliance with FISMA requirements to Congress. The FY 2016 IG FISMA Reporting Metrics requires agencies to provide their annual FY 2016 FISMA Metrics by November 10, 2016. OMB's principal written statement of Government policy regarding information security is OMB Circular No. A-130, Appendix I, *Responsibilities for Protecting and Managing Federal Information Resources*, dated July 28, 2016, which establishes a minimum set of controls to be included in Federal automated Information Security Programs. In particular, OMB Circular A-130, *Managing Information as a Strategic Resource*[8] defines adequate security as, "Security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls."

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 PUBs 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***. Each security control family includes controls associated with the security functionality of the family.

[8] OMB Circular A-130 is available at https://www.whitehouse.gov/omb/circulars_default.

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 has categorized information systems 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, the Corporation categorized all as having a moderate or low security impact.

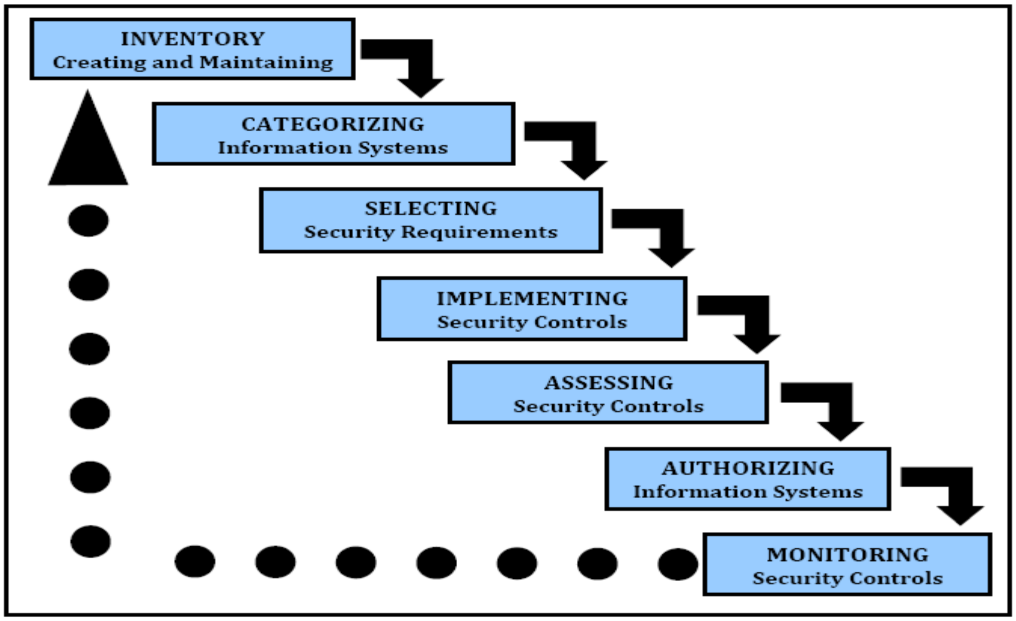
The Corporation has adopted guidance from NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, for authorizing its systems. The NIST Risk Management Framework (RMF) comprises the following six steps and provides a structured 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 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 FISMA Metrics*, *Senior Agency Official for Privacy FISMA Reporting Metrics*, and *OIG FISMA 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 2016 IG FISMA of 2014 Reporting Metrics* and requires each agency OIG to respond to FISMA metric questions in eight metric domains. ***Exhibit 5: Summary of FY 2016 IG FISMA Responses/Comparison to***

FY 2015 Results in Section 3 shows the new IG FISMA metrics structure, the corresponding FY 2016 metric domains, and Kearney's test results.

2.4 Scope

Kearney conducted an independent evaluation of the Corporation's Information Security Program from May through September 2016 at CNCS headquarters in Washington, D.C. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation*, promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE), and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

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, two major applications (eSPAN and Momentum), and VISTA Healthcare Benefits (VHB) for compliance with selected NIST SP 800-53, Rev. 4 controls. In addition to the eight FISMA metric domains, Kearney tested the Corporation's privacy controls.

The FISMA evaluation included an assessment of the following:

- Site visits to the Corporation State Office (Seattle, WA) and the AmeriCorps Pacific NCCC Region in Sacramento, California
- The Corporation's Information Security Program and privacy controls
- Management oversight of contractor-managed systems, including the Corporation's GSS and eSPAN.

3. RESULTS

This section provides the conclusions of Kearney's research, analysis, and assessment of the Corporation's information security program, policies, and practices. We included a summary of the new maturity levels and criteria for program effectiveness that the Council of the Inspectors General on Integrity and Efficiency (CIGIE) Federal Audit Executive Council (FAEC) IT Working Group established for the FY 2016 IG FISMA Reporting Metrics. In addition, we presented a summary of the FY 2016 IG FISMA Reporting Metrics responses, provided to the OIG as a separate deliverable. We compared the metric results from our FY 2016 assessment with the FY 2015 results and noted the areas where the Corporation has improved by closing 67 prior-year recommendations and eight of seventeen findings. While positive, continued management attention is necessary as Kearney identified that the Corporation was noncompliant with OMB guidance and NIST SPs in 25 of 57 security metrics found in six of eight non-maturity model domains. In the following subsections, we present the findings from our testing of the Corporation's systems.

Maturity Model Results

For the two domains utilizing maturity models, ISCM and IR, Kearney determined that the Corporation achieved a maturity rating of Level 2: *Defined* for People, Processes, and Technology. The CIGIE FAEC IT Working Group established five levels of maturity for Information Security Programs in the FY 2016 IG FISMA Reporting Metrics, as shown in ***Exhibit 3***.

Exhibit 3: Maturity Levels and Definitions

Maturity Level and Title	Brief Definition
Level 1: Ad-hoc	Program is not formalized. Activities are performed in a reactive manner.
Level 2: Defined	Program is formalized, but policies, plans, and procedures are not consistently implemented organization-wide.
Level 3: Consistently Implemented	Formalized program is consistently implemented across the agency, but measures of effectiveness are not captured and used.
Level 4: Managed and Measurable	Program activities are repeatable and metrics are used to measure and manage program implementation, achieve situational awareness, and control ongoing risk.
Level 5: Optimized	Program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis due to changes in business/mission requirements, as well as a changing threat and technology landscape.

For FY 2016, using the five maturity levels above, DHS instituted a scoring system through CyberScope for determining the degree of maturity of agency Information Security Programs, as well as specific criteria to determine whether the agency's program in each metric domain was effective. For the six metric domains without maturity models, The DHS CyberScope reporting assigned a "maturity model indicator," corresponding each metric to one of three maturity levels (2, 3, or 4). For the two metric domains with maturity models in the FY 2016 IG FISMA Reporting Metrics, the CIGIE FAEC IT Working Group requires that all metrics at lower levels, as well as greater than 50 percent at the rated level (e.g., Level 2, Level 3, etc.), must be met in order to achieve that level. The CIGIE FAEC IT Working Group further stipulates that a security program must achieve at least the "*Managed and Measurable*" level to be considered effective.

Based on the IG's assessment of whether each individual metric was "met" or "not met," a score is computed for each of the five information security functions in the Cybersecurity Framework. For those functions that include more than one metric domain, the results for the individual metrics in the domains are combined to determine the score for that function. Agencies are allotted points for each Cybersecurity Framework function area based on their achievement of various levels of maturity. For each framework function, a total of 20 points is possible. The Corporation's scores are shown in ***Exhibit 4***. For FY 2016, the Corporation scored 37 points out of 100 possible.

Exhibit 4: Corporation's Cybersecurity Framework Function Scorecard

Function Area	Level	Points	Possible
Identify	Level 3: *Consistently Implemented*	13	20
Protect	Level 2: *Defined*	7	20
Detect	Level 2: *Defined*	7	20
Respond	Level 2: *Defined*	7	20
Recover	Level 1: *Ad hoc*	3	20
Total		**37**	**100**

In addition to calculating an IG FISMA metric score, Kearney compared the test results from FYs 2015 to 2016 to measure the Corporation's progress. As ***Exhibit 5*** illustrates, six of the eight domains evaluated warrant additional management attention to address identified deficiencies. In addition to evaluating the *FY2016 IG FISMA Metrics*, Kearney also tested eight privacy controls from NIST SP 800-53 Rev. 4 and noted the Corporation had successfully implemented these controls. Accordingly, Kearney closed seven prior year recommendations related to privacy.

To determine the severity of noted exceptions, we 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 eight FISMA metric domains. Kearney's responses to the *FY 2016 IG FISMA Reporting Metric* questions are contained in a separate deliverable to the OIG.

Exhibit 5: Summary of FY 2016 IG FISMA Responses/Comparison to FY 2015 Results

FY 2016 IG FISMA Metric Domain (Security Function)	2015: # of DHS Exceptions/ Total DHS IG Security Metric Questions[9]	2016: # of DHS Exceptions/ Total DHS IG Security Metric Questions	Controls Effective Overall (Yes/No)	2016: Severity of Noted Exceptions
1.1 Risk Management (Identify), includes FY 2015 POA&M[10]	Risk Management: 9 of 16 POA&M: 6 of 9	2 of 16	No	Control Deficiency
1.2. Contractor Systems (Identify)	4 of 8	2 of 3	No	Control Deficiency
2.1 Configuration Management (Protect)	9 of 12	6 of 9	No	Control Deficiency
2.2 Identity &Access Management (I&AM) (Protect), includes FY 2015 Remote Access[11]	I&AM: 1 of 9 Remote Access Management: 3 of 12	8 of 14	No	Control Deficiency
2.3 Security and Privacy Training (Protect)	3 of 7	2 of 5	No	Demonstrates Effectiveness
3.1 ISCM (Detect)[12]	Level 2 for People, Processes, and Technology	People, Processes, and Technology Assessed at Level 2: Defined	Yes	Control Deficiency
4.1 Incident Response (Respond)[13]	Incident Response: 2 of 8	People, Processes, and Technology Assessed at Level 2: Defined	Yes	Control Deficiency
5.1 Contingency Planning (Recover)	10 of 12	5 of 10	No	Control Deficiency

[9] For maturity models, results indicate the level for each of the three areas. The overall level is the lowest area level.

[10] DHS merged the Risk Management and POA&M domains in FY 2016.

[11] DHS merged the I&AM and Remote Access domains in FY 2016.

[12] DHS provided a maturity model for ISCM for both FY 2015 and FY 2016.

[13] DHS provided individual metrics for IR in FY 2015 and a maturity model in FY 2016.

In addition to comparing FISMA results from FY 2015 to FY 2016, we prepared ***Exhibit 6*** to highlight the two new findings from FY 2016 and the nine open findings from the prior FYs 2013, 2014, and 2015 FISMA evaluations.

Exhibit 6: Summary of Open FISMA Findings

NIST Cyber-security Domain	NFR Description	Remediation Status	Open Recommend-ations	Severity
Identify	1. Inadequate Enterprise-Wide Risk Management Policies and Practices *(FY 14 - FISMA - NFR 9)*	In Progress	3 of 4	Control Deficiency
Identify	2. Weaknesses with the Corporation's Security Planning and Assessment Process *(FY 14 - FISMA - NFR 10)*	In Progress	6 of 13	Control Deficiency
Identify	3. Improvements Needed to POA&M Reporting *(FY 14 - FISMA - NFR 12)*	Closed	0 of 3	Closed
Protect	4. Risks to the Confidentiality and Availability of Voice Communications *(FY 14 - FISMA - NFR 6)*	In Progress	2 of 5	Control Deficiency
Protect	5. Secure Configuration Management Policies, Procedures, and Practices Need Improvement *(FY 16 – FISMA - NFR 1)*	New	5 of 5	Control Deficiency
Protect	6. Lack of Formal, Role-Based Training *(FY 14 - FISMA - NFR 11)*	Closed	0 of 3	Closed
Protect	7. Inadequate Controls over Remote Access *(FY 14 - FISMA - NFR 13)*	In Progress	1 of 3	Control Deficiency
Protect	8. Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement *(FY 15 - FISMA - NFR 2)*	In Progress	2 of 3	Control Deficiency
Detect	9. Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy (*FY 14 - FISMA - NFR 1*)	In Progress	2 of 8	Control Deficiency
Detect	10. Multiple Weaknesses with Vulnerability Scanning and Remediation (*FY 14 - FISMA - NFR 2*)	In Progress	6 of 12	Control Deficiency
Detect	11. Organizational Conflict of Interest (*FY 14 - FISMA - NFR 3*)	Closed	0 of 3	Closed
Detect	12. Use of an Obsolete and Unsupported Network Monitoring Tool *(FY 14 - FISMA - NFR 4)*	Closed	0 of 6	Closed
Detect	13. Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses *(FY 15 - FISMA - NFR 1)*	Closed	0 of 6	Closed
Detect	14. Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan *(FY 15 - FISMA - NFR 3)*	Closed	0 of 6	Closed
Recover	15. Inadequate Disaster Recovery Plan (DRP) Documentation and Planning *(FY 14 - FISMA - NFR 14)*	In Progress	5 of 5	Control Deficiency
Recover	16. Lack of Adequate Testing of Continuity of Operations Plan (COOP) *(FY 14 - FISMA - NFR 15)*	Closed	0 of 4	Closed

NIST Cyber-security Domain	NFR Description	Remediation Status	Open Recommend-ations	Severity
Recover	17. Inadequate Controls over Privacy Data *(FY 14 - FISMA - NFR 16)*	Closed	0 of 7	Closed
Recover	18. Inaccurate Inventory of Physical Information Technology Asset *(FY 15 - FISMA - NFR 4)*	In Progress	1 of 4	Control Deficiency
Recover	19. Insufficient Monitoring and Remediation of Server Backup Failures *(FY 16 – FISMA -NFR – 2)*	New	3 of 3	Control Deficiency
Open Recommendations from consolidated FY 2014, 2015, and 2016			**36**[14]	

Kearney's testing resulted in two new findings and 13 additional recommendations. Five of the 13 new recommendations relate to prior year finding FY 14 – FISMA – NFR 2 *Multiple Weaknesses with Vulnerability Scanning and Remediation*. These new findings are described in Appendix A, while nine of the 17 findings from the FY 2015 FISMA evaluation were repeated or updated, as described in Appendix B: Status of Prior-Year Findings. During the FY 2016 evaluation, the Corporation addressed 67 of 90[15] prior year recommendations from the FY 2014 and 2015 FISMA evaluations by implementing corrective actions or signing risk acceptance waivers, while 23 recommendations from prior years remain open and are repeated. In most instances, the Corporation had corrective actions in progress at the close of the FY 2016 FISMA evaluation to address the outstanding recommendations.

[14] Of the 36 open recommendations, 20 are open recommendations from FY 2014, three are open recommendations from FY 2015, and 13 are open recommendations from FY 2016.

[15] Of the total 90 prior year recommendations that were open at the beginning of the FY 2016 FISMA evaluation, 51 prior year recommendations from FY 2014 and 16 prior year recommendations from 2015 were "Closed" (51+16=67). In addition to the 90 prior-year recommendations, Kearney added five new recommendations to *FY 14 - FISMA - NFR 2*.

APPENDIX A: FY 2016 NEW FINDINGS – NOTIFICATIONS OF FINDINGS AND RECOMMENDATIONS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") issued two Notifications of Findings and Recommendations (NFR) to the Corporation for National and Community Service (the Corporation) as a result of the fiscal year (FY) 2016 Federal Information Security Modernization Act of 2014 (FISMA) Independent Evaluation. The two new NFRs are listed and described below.

Cybersecurity Framework Domain: ***Protect***
FY 16 FISMA IG Metric Area: ***Configuration Management (CM)***

1. Subject: Secure Configuration Management Policies, Procedures, and Practices Need Improvement (FY16 – FISMA – NFR 1)

Background: The establishment and distribution of documented configuration management (CM) policies and procedures is essential to consistently implement security controls for the protection of Government systems and data. Policies and procedures establish expectations for how an agency and its contractors implement and maintain configuration management controls and become more important when contractors play a leading role in maintaining configuration baselines and tracking deviations.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and Organizations, requires Federal organizations to develop, document, review, and update current CM policy and procedures in security control CM-1 Configuration Management Policy and Procedures for information systems with a FIPS-199 moderate and low impact rating. Further, CM-2 Baseline Configuration explains the concept of configuration baselines as a "documented, formally reviewed and agreed-upon sets of specifications for the information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems." In addition, security control CM-9 Configuration Management Plan requires information systems to establish a CM plan to: address roles, responsibilities, and processes and procedures; establish a process to identify configuration items (CI) throughout the system development lifecycle (SDLC) and manage the configuration of the CIs; and define the CIs for the information system and place the CIs under CM. Finally, NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, provides further instructions on implementing CM controls outlined in NIST SP 800-53.

During the fiscal year (FY) 2016 Federal Information Security Modernization Act of 2014 (FISMA) evaluation for the Corporation for National and Community Service (CNCS), Kearney & Company, P.C. (Kearney) noted that CNCS defined various CM control requirements for the agency and its IT contractors. Kearney also noted that CNCS's Managed IT Services (MITS) contractor was responsible for conducting weekly, authenticated vulnerability scans of CNCS's desktops, servers, switches, routers, and wireless access points to confirm that the devices were securely configured using the baselines configuration and appropriate security patches were installed.

Condition: Kearney identified the following two deficiencies with CNCS's CM practices:

1. *Incomplete CM Plan, Policies, and Procedures*

Kearney validated that CNCS's Office Information Technology (OIT) CM plan is still draft as of August 29, 2016 and lacks important details to establish effective policies and procedures that ensure compliance with minimally acceptable system configuration requirements (e.g., baseline settings, IT asset and infrastructure management, and configuration item definitions, descriptions, and processes) to identify and track approved deviations. Kearney observed that the draft CM plan did not incorporate guidance from NIST SP 800-128 and describe practices for tracking configuration items, deviations from secure configuration baselines, and results from security impact analysis (SIA). CNCS began the process of developing the Office of Information Technology (OIT) CM plan in October 2015 by defining scope of the plan; however, CNCS does not plan to complete the missing sections of the CM plan until December 2016.

2. *Secure Configuration Baseline System Settings for CNCS's GSS Devices are not Documented, Approved, and Fully Implemented across the GSS*

CNCS has selected a secure configuration baseline standard, the United States Government Configuration Baseline (USGCB), for its desktops. However, the Corporation and its MITS contractor have not documented the approved deviations from the USGCB settings in a centralized document or electronic repository.

For Windows servers, similar challenges exist. While the Corporation has implemented Group Policy Object (GPO) settings for its Windows servers that are members of the Corporation's Active Directory domain, the Corporation has not established and documented a "standard Windows server" configuration that includes these GPO settings and the included software, software versions, and configurations. Additionally, Windows servers, not part of the Corporation's Windows Active Directory domain, do not receive these GPO settings. Specifically, Kearney noted the following CM weaknesses on servers:

- The CNCS Blade Server Build Guide document did not detail configuration settings and
- The CNCS Virtual Machine (VM) Server Build Guide document did not detail configuration settings.

For both desktops and servers, the Corporation has not centrally maintained and documented its approved deviations from a configuration baseline as the desktop and server configuration baselines changed over time. Further, the Corporation has not implemented a monitoring and remediation process to identify and correct deviations from its approved configuration baselines for both desktops and servers.

Finally, although CNCS' MITS contractor performs weekly vulnerability scans of desktops and servers, the MITS contractor does not utilize the vulnerability scan results to identify and correct deviations from the desktop and server baselines.

Criteria: CNCS establishes IT security policies and procedures parameters in its Cybersecurity Controls Family document, which incorporates NIST SP 800-53, Rev. 4 security and privacy controls and documents CNCS's assignment of responsibility.

For CM-1 Configuration Management Policy and Procedures, CNCS's Cybersecurity Controls Family states:

> "a. The Chief Information Security Officer (CISO) is responsible for:
> (1) Developing, documenting, and disseminating a configuration management policy to individuals with system security responsibilities that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
> (2) Reviewing and updating the current configuration management policy annually.
>
> b. The Information System Security Officer (ISSO) is responsible for:
> (1) Developing, documenting, and disseminating procedures to facilitate the implementation of the configuration management policy and configuration management controls; and
> (2) Reviewing and updating the current configuration management procedures annually."

Regarding additional CM controls, the Cybersecurity Controls Family document states the following for CM-2 Baseline Configuration:

> "The ISSO, in accordance with the configuration management policy, is responsible for developing, documenting, and maintaining under configuration control, a current baseline configuration of the information system.
>
> a. The ISSO is responsible for:
> (1) BASELINE CONFIGURATION | REVIEWS AND UPDATES
> Reviewing and updating the baseline configuration of the information system:
> (a) Annually;
> (b) When required due to changes or updates to the system; and
> (c) As an integral part of information system component installations and upgrades.
> (3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS
> Retaining older versions of baseline configurations as deemed necessary to support rollback.
> (7) BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS

(a) Mobile devices are issued with more stringent configuration settings to individuals traveling to locations that the Corporation deems to be of significant risk; and

(b) Reviewing for signs of physical tampering and purging/reimaging is performed to the devices when the individuals return."

Cause: CNCS has not prioritized the development and documentation of CM policies, procedures, and plans to incorporate the security-focused configuration management requirements from NIST SP 800-53, Rev. 4 and NIST SP 800-128. CNCS has signed a long-term IT outsourcing agreement and generally expects its MITS provider to adhere to FISMA, Office of Management and Budget (OMB), and NIST security mandates, including requirements to develop and maintain a security-focused CM plan. The MITS contract requires its vendor to provide an Information System Security Officer (ISSO) to implement and monitor NIST SP 800-53 security controls, including the required CM controls. However, CNCS's oversight and ongoing monitoring of its MITS contractor did not identify these weaknesses regarding CM policies and procedures in the GSS Plan of Action and Milestones (POA&M) or encourage its MITS contractor to correct such weaknesses timely, if they were known. Regarding configuration baselines, the Corporation's CM program has not matured to document a configuration baseline for desktops and servers and then track approved deviations from USGCB or the Corporation's Windows server baseline for both member and non-member Windows domain servers. Further, while Corporation collects and approves change requests using the Technical Review Board (TRB), it does not update its configuration baselines for desktop and servers when such changes are approved. Finally, while the Corporation's MITS contractor performs weekly vulnerability scans, the Corporation's MITS contractor has not configured and implemented a "configuration focused" scan to identify deviations from the Corporation's baselines for desktops, servers, and other network devices.

Effect: Without clearly defined and implemented CM policies, procedures, and a CM plan, CNCS cannot obtain assurance that information system settings are securely configured and implemented. Likewise, MITS contractor personnel, who implement configuration settings on desktops and servers, do not have clear guidance of expected settings and awareness of approved deviations from the baseline when new desktops and servers are deployed to development, test, and production environments. Lacking clear guidance from CNCS, the MITS contractor cannot develop a "configuration scan profile" (e.g. tailored Nessus plugin) to detect desktop and server deviations from the Corporation's configuration baselines. Under these circumstances, CNCS may experience unplanned IT outages or insecure configurations may be deployed to production.

Recommendations: Kearney recommends that the Corporation:

1. Update and implement the draft CM plan to incorporate security-focused configuration management requirements from NIST SP-800 53, Rev. 4 (i.e., controls CM-1 to CM-9) and NIST SP 800-128.
2. Establish and document the Corporation's secure configuration baseline for desktops and servers. Consider guidance from NIST SP 800-70 Rev. 3 *National Checklist Program*

for IT Products and external sources such as Microsoft and the Center for Internet Security for the development of secure configuration baselines.

3. Implement a process to maintain configuration baselines for desktops, servers and other network equipment that records installed software, software versions, and configuration settings as required by NIST SP 800-53, CM-2 *Baseline Configuration*.
4. Improve TRB CM procedures by implementing a process to document and track deviations from approved configuration baselines, as required by CM control *CM-3 Configuration Change Control*. As part of the process, ensure deviations from the configuration baselines are documented with business justification.
5. Perform periodic configuration scans to identify deviations from the Corporation's configuration baselines for desktops, servers, and network equipment. The objective of the configuration scans should be to identify deviations (i.e., missing or outdated antivirus software, missing backup agents, non-standard software or settings) from the approved configuration baseline in contrast to other scans designed to identify missing security patches and other vulnerabilities.

Cybersecurity Framework Domain: ***Recover***
FY 16 FISMA IG Metric Area: ***Contingency Planning***

2. Subject: Insufficient Monitoring and Remediation of Server Backup Failures (FY16 – FISMA – NFR 2)

Background: Information system backups provide the Corporation and their users with the ability to restore their data and files in the event of a hardware failure or security incident (e.g., ransomware). Backup frequencies are aligned to recovery strategies developed from Business Impact Analysis (BIA) and contingency plan requirements in order to minimize potential data loss and to aid in the timely recovery of the information system. The Managed Information Technology Services (MITS) contractor, supporting the Corporation for National and Community Service (the Corporation), is responsible for configuring, managing, and monitoring data backups on the Corporation's General Support System (GSS).

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and Organizations, CP-9 Information System Backup, emphasizes the requirements for Federal agencies to backup data at the user level, system level, and information system. The Corporation's Cybersecurity Control Families document (CFD) identifies how the Corporation implements the NIST SP 800-53 controls. CP-9 Information System Backup states that the Information System Security Officer (ISSO) is responsible for ensuring backups of user-level, system-level, and information system documentation are performed and are consistent with the requirements in the contingency plans. Additionally, the Corporation states that backup information must be tested at least annually to verify media reliability and information integrity.

As part of the fiscal year (FY) 2016 Federal Information Security Modernization Act of 2014 (FISMA) evaluation, Kearney & Company, P.C. (Kearney) tested the Corporation's Contingency Planning controls over its GSS and reviewed its server backup practices. According to the GSS's System Security Plan (SSP):

> "Backups must be performed with the following frequency:
>
> - Full backups of Corporation Headquarter (HQ) data is performed on a weekly basis (beginning on Fridays)
> - Incremental and differential backups are performed between Monday through Thursday
> - Data archives are transported offsite with daily backups (Monday through Thursday) when storage media is full
> - Storage Area Network (SAN)-to-SAN replication to the alternate processing site occurs in "near-real-time."

During an interview with Kearney, the MITS contractor explained that its practice is to remediate failed backup jobs within 24 hours. Additionally, the Corporation and its MITS contractor considers backup jobs that return a message code of "The requested operation was partially successful” as a successful backup.

Condition: Kearney tested the Corporation’s oversight and monitoring of server backups of the GSS. Of the 2,852 GSS backup jobs that were logged between July 9, 2016 and September 6, 2016, 9.13 percent (260) did not successfully complete a backup to one of the three configured media servers on the first attempt. While a limited number of backup job failures is expected on a periodic basis and can be explained by complexities of the information technology (IT) environments and operations, Kearney’s review of the backup logs identified that subsequent backup jobs often took a significant amount of time to correct. Of the 260 jobs that failed, network connection and configuration errors caused 43.08 percent (112) and 41.54 percent (108) respectfully while 15.38 percent (40) of the failures were caused by file access related issues. Table 1 below provides error messages received when a noted server backup job failed.

Table 1: GSS Backup Job Outcomes between July 9, 2016 and September 6, 2016

Backup Job Results – Failure & Success Codes	Error Type	Count of Description	Percent
Network read failed	Network	1	0.04%
Media open error	Access	2	0.07%
Client hostname could not be found	Configuration	3	0.11%
No storage units available for use	Configuration	6	0.21%
Access to the client was not allowed	Access	8	0.28%
File read failed	Access	9	0.32%
Snapshot error encountered	Configuration	12	0.42%
File write failed	Access	21	0.74%
Network connection timed out	Network	33	1.16%
Client backup was not attempted because backup window closed	Configuration	36	1.26%
POLICY Catalog SCHED Full EXIT STATUS 0 (the requested staging operation was successfully completed)	Configuration	51	1.79%
Can't connect to client	Network	78	2.73%
Subtotal of Backup Error Messages		260	9.13%
*The requested operation was partially successful	N/A	471	16.51%
The requested operation was successfully completed	N/A	2,121	74.37%
Grand Total		**2,852**	**100%****

***Note**: Partially successful backup jobs occur when individual files are locked at the time of backup and are not included in the backup as a result. The Corporation considers partially successfully backup jobs to be successful.
** Percentage may not total to 100% due to rounding.

Criteria: FISMA, Public Law (P.L.) 113-283 § 3554, documents Federal agency responsibilities to include:

> "(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— …
>
> (8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."

Per the Corporation's CFD, NIST SP 800-53, Rev. 4, CP-9 *Information System Backup*:

> "The ISSO is responsible for ensuring:
>
> a. Backups of user-level information contained in the information system are conducted ***and consistent with the requirements in the system operating and contingency plans****;*
> b. Backups of system-level information contained in the information system are conducted ***and consistent with the requirements in the system operating and contingency plans*****;**
> c. Backups of information system documentation including security-related documentation are conducted ***and consistent with the requirements in the system operating, contingency plans*****;** and
> d. The confidentiality and integrity of backup information at the storage location is protected.
>
> **Control Enhancements:**
> The ISSO is responsible for ensuring:
> *(1) INFORMATION SYSTEM BACKUP | TESTING FOR RELIABILITY / INTEGRITY*
> Backup information is tested ***at least annually*** to verify media reliability and information integrity."

Cause: Discussions with the Corporation's MITS contractor revealed that the contractor's system administrators did not consistently investigate and resolve instances when backup jobs failed. The supervisor for the system administrators and the Corporation did not identify repeated failures through secondary review of backup logs. Lastly, the Corporation had not established a service level agreement (SLA) or performance measure related to the completion of successful backups and remediation of any identified errors.

Effect: Without ensuring that backups are successful and failures are remediated, the Corporation is at risk of losing data and / or untimely system restoration in the event of a critical disaster or a serious security incident. Security incidents, such as the ransomware (i.e., Loki virus) that struck the Corporation on March 29, 2016 and encrypted users' files on the S: Drive, highlight the importance of frequent server backups as the Corporation used these backups to recover encrypted files.

Recommendations: Kearney recommends that the Corporation:

1. Develop and implement a process to monitor GSS backup jobs for failures, particularly for backup jobs identified as critical. Consider utilizing automated alerts and developing naming conventions for server backup jobs identified as "critical" backups to ensure prompt, corrective action is taken by responsible individuals. Update the GSS SSP to reflect the new monitoring process for backup jobs.
2. Investigate backup job failures when they continue to occur to determine the root cause and remedial solutions.
3. Develop a service level agreement (SLA) or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements

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 Notifications of Findings and Recommendations (NFR) reported in the *Federal Information Security Management Act Independent Evaluation for Fiscal Year (FY) 2014*, Office of Inspector General (OIG) Report 15-03[16] and the *FY 2015 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service (CNCS)*, OIG Report 16-03.[17] From FY 2014 and 2015 FISMA evaluations, the Corporation implemented corrective actions or signed risk acceptance waivers to close eight prior year findings and addressed 67 of 90[18] prior year recommendations. Kearney identified new weaknesses with the Corporation’s vulnerability scanning and remediation practices and added five new recommendations to FY 14 FISMA NFR 2. ***Exhibit 7*** presents a summary of the resolution status for each NFR from FYs 2013, 2014, and 2015.

Exhibit 7: Resolution Status of FYs 2013, 2014, and 2015 NFRs

FISMA NFRs	FY 13 Finding	FY 14 Severity	FY 15 Severity	FY 16 Severity	FY 16 Status	Closed Recs	Open Recs	Total Recs
1. Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy (*FY 14 - FISMA - NFR 1*)	X	Significant Deficiency	Significant Deficiency	Control Deficiency	In Progress	6	2	**8**
2. Multiple Weaknesses with Vulnerability Scanning and Remediation (*FY 14 - FISMA - NFR 2*)	N/A	Significant Deficiency	Significant Deficiency	Control Deficiency	In Progress	6	6[19]	**12**
3. Organizational Conflict of Interest (*FY 14 - FISMA - NFR 3*)	N/A	Significant Deficiency	Significant Deficiency	N/A	Closed	3	0	**3**

[16] For the full text of the FY 2014 FISMA report, visit http://www.cncsoig.gov/sites/default/files/15-03_0.pdf.
[17] For the full text of the FY 2015 FISMA report, visit https://www.cncsoig.gov/sites/default/files/16-03.pdf.
[18] In addition to the 90 prior-year recommendations, Kearney added five recommendations to FY 2014 NFR #2.
[19] Five new recommendations were added to FY 14 – FISMA – NFR 2 as a result of testing, bringing the total number of recommendations Closed to 6, Open to 6, and the Total to 12.

FISMA NFRs	FY 13 Finding	FY 14 Severity	FY 15 Severity	FY 16 Severity	FY 16 Status	Closed Recs	Open Recs	Total Recs
4. Use of an Obsolete and Unsupported Network Monitoring Tool *(FY 14 - FISMA - NFR 4)*	N/A	Significant Deficiency	Significant Deficiency	N/A	Closed	6	0	**6**
5. FY 2014 Finding #6: Risks to the Confidentiality of Voice Communications	N/A	Significant Deficiency	Significant Deficiency	Control Deficiency	In Progress	3	2	**5**
6. **Inadequate Enterprise-Wide Risk Management Policies and Practices *(FY 14 - FISMA - NFR 9)***	X	Control Deficiency	Control Deficiency	Control Deficiency	In Progress	1	3	**4**
7. Weaknesses with the Corporation's Security Planning and Assessment Process *(FY 14 - FISMA - NFR 10)*	X	Significant Deficiency	Significant Deficiency	Control Deficiency	In Progress	7	6	**13**
8. Lack of Formal, Role-Based Training *(FY 14 - FISMA - NFR 11)*	X	Control Deficiency	Control Deficiency	N/A	Closed	3	0	**3**
9. Improvements Needed to POA&M Reporting *(FY 14 - FISMA - NFR 12)*	X	Significant Deficiency	Control Deficiency	N/A	Closed	3	0	**3**
10. Inadequate Controls over Remote Access *(FY 14 - FISMA - NFR 13)*	N/A	Control Deficiency	Control Deficiency	Control Deficiency	In Progress	2	1	**3**

FISMA NFRs	FY 13 Finding	FY 14 Severity	FY 15 Severity	FY 16 Severity	FY 16 Status	Closed Recs	Open Recs	Total Recs
11. Inadequate Disaster Recovery Plan (DRP) Documentation and Planning *(FY 14 - FISMA - NFR 14)*	N/A	Control Deficiency	Control Deficiency	Control Deficiency	In Progress	0	5	**5**
12. Lack of Adequate Testing of Continuity of Operations Plan (COOP) *(FY 14 - FISMA - NFR 15)*	N/A	Control Deficiency	Control Deficiency	N/A	Closed	4	0	**4**
13. Inadequate Controls over Privacy Data *(FY 14 - FISMA - NFR 16)*	N/A	Significant Deficiency	Control Deficiency	N/A	Closed	7	0	**7**
14. Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses *(FY 15 - FISMA - NFR 1)*	N/A	N/A	Significant Deficiency	N/A	Closed	6	0	**6**
15. Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement *(FY 15 - FISMA - NFR 2)*	N/A	N/A	Control Deficiency	Control Deficiency	In Progress	1	2	**3**

FISMA NFRs	FY 13 Finding	FY 14 Severity	FY 15 Severity	FY 16 Severity	FY 16 Status	Closed Recs	Open Recs	Total Recs
16. Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan *(FY 15 - FISMA - NFR 3)*	N/A	N/A	Control Deficiency	N/A	Closed	6	0	**6**
17. Inaccurate Inventory of Physical Information Technology Asset *(FY 15 - FISMA - NFR 4)*	N/A	N/A	Control Deficiency	Control Deficiency	In Progress	3	1	**4**
Total						**67**	**28**	**95**

FY 2014 – FISMA – NFR 1: Lack of a Formally Documented and Fully Implemented ISCM Strategy[20]

In 2014, Kearney reported that the Corporation had not formally documented and implemented an organization-wide ISCM Program and strategy, as mandated by the Office of Management and Budget (OMB) guidance and 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 (Rev.) 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, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

During the 2015 FISMA evaluation, Kearney reported similar weaknesses associated with developing and implementing the Corporation’s ISCM process. The Corporation cited resource constraints as precluding it from developing and implementing an ISCM Program prior to filling various key IT position vacancies. The Corporation had taken a number of important steps to address the prior-year weaknesses. These steps included 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)[21] Program.

While these developments were positive, weaknesses remained at the close of the 2015 FISMA evaluation of the Corporation’s ISCM Program. The Corporation had only an incomplete draft ISCM strategy that contained multiple highlights and reviewer comments, demonstrating that additional work was needed. Kearney confirmed that the draft ISCM strategy did not identify performance metrics that were meaningful and reportable for all business processes supporting the Corporation’s mission. In 2015, Kearney assessed the Corporation’s ISCM Program as Level 1: *Ad Hoc* in each of the three required evaluation areas (i.e., People, Processes, and Technology).

FY 2016 Update:

In the FY 2016 FISMA evaluation, Kearney noted that the Corporation made improvements to the ISCM Program by implementing six of the eight prior-year recommendations.

[20] For text of this prior-year finding, please refer to page 40 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. Additional details from the FY 2014 FISMA evaluation are available in OIG Report 15-03.

[21] 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.

FY 2014 – FISMA – NFR 1: Lack of a Formally Documented and Fully Implemented ISCM Strategy[20]

Specifically, the Corporation formally documented and implemented an organization-wide ISCM strategy that considered risk at the Tier 1: Organization and Tier 2: Business Process levels. In April 2016, the Corporation hired a Chief Risk Officer (CRO), who initiated a process to identify, classify, and review organizational risks to the Corporation's mission and business processes. As part of the ISCM strategy, the Corporation established frequencies (i.e., daily, weekly, monthly) for performing specific security control monitoring activities (e.g., monthly reviews of inactive user accounts). Examples of monitoring activities include weekly Operations meetings with the Managed IT Service (MITS) contractor, biweekly review of the Plans of Action and Milestones (POA&M), and weekly reviews of vulnerability scan results. Other improvements for FY 2016 included reporting the status of POA&M remediation activities to the Executive Steering Committee and implementation of Service Level Agreements (SLA) with the Corporation's MITS contractor.

The Corporation also completed a full security control assessment of its general support system (GSS), but it did not complete annual security control testing for Momentum, its financial system, or eSPAN. As a result, the security status of these systems was not reported to Office of Information Technology (OIT) and Corporation executives. In addition, the Corporation installed a Security Information Event Management (SIEM) solution, Splunk,[22] to provide the ability to correlate and analyze audit log events from multiple servers. While the initial implementation was successful, the Corporation only succeeded in using Splunk to monitor a small number of monitoring scenarios. The Corporation plans to leverage more of Splunk's out-of-the-box capabilities to design a robust monitoring program.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 1 – Rec #1: Document and fully implement an organization-wide, comprehensive ISCM strategy that incorporates Tier 1 and Tier 2 levels	In Progress	Closed
FY 2014 – FISMA – NFR 1 – Rec #2: Improve oversight over IT service providers	In Progress	Closed
FY 2014 – FISMA – NFR 1 – Rec #3: Formalize ISCM processes to include the following:	N/A	N/A
FY 2014 – FISMA – NFR 1 – Rec #3 – Part A: Establishment of metrics to be monitored	In Progress	Closed
FY 2014 – FISMA – NFR 1 – Rec #3 – Part B: Establishment of frequencies for monitoring/assessments	In Progress	Closed
FY 2014 – FISMA – NFR 1 – Rec #3 – Part C: Approach for ongoing security control assessments and status monitoring to determine the effectiveness of deployed security controls	In Progress	Closed

[22] Splunk is an appliance that captures, indexes, and correlates real-time data in a searchable repository from which users can generate graphs, reports, alerts, dashboards, and visualizations.

FY 2014 – FISMA – NFR 1: Lack of a Formally Documented and Fully Implemented ISCM Strategy[20]		
FY 2014 – FISMA – NFR 1 – Rec #3 – Part D: Correlation and analysis of security-related information generated by assessments and monitoring	In Progress	In Progress
FY 2014 – FISMA – NFR 1 – Rec #3 – Part E: Response actions to address the results of the analysis	In Progress	In Progress
FY 2014 – FISMA – NFR 1 – Rec #3 – Part 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	Closed

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]

In FY 2014, 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, thus allowing 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)[24]
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, Rev. 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.

Lack of Performance Metrics
During FY 2015, the Corporation took 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.[25]

Completeness and Accuracy of Scan Results
Weaknesses remained 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

[23] For text of this prior-year finding, please refer to page 43 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. The full text of the prior-year finding is available in OIG Report 15-03.
[24] 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 Security Content Automation Protocol (SCAP).
[25] See related FY 2015 FISMA finding: *Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses* in the OIG report 16-03.

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]
patches from August 2014 through December 2014 when it deployed Microsoft Office 365.[26] 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 SCAP.[27] 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[28] • 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

[26] Microsoft Office 365 is a group of software plus services subscriptions that provides productivity software, such as e-mail and SharePoint, to its subscribers.

[27] SCAP is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

[28] 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.

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]
• eSPAN servers contained 58 high-risk vulnerabilities. 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.
2016 Update: The Corporation has taken steps to resolve six of the seven open prior-year weaknesses. These steps include establishing performance metrics to resolve identified security vulnerabilities by risk (i.e., critical, high, moderate, or low). The Corporation's MITS contractor, in coordination with OIT, is required to remediate identified security vulnerabilities within specific timeframes (e.g., critical – 30 days, high – 60 days, moderate – 90 days, etc.) or add the vulnerability to the system POA&M for tracking. Other positive steps include replacing the unsupported vulnerability scanner with a new one, performing authenticated scans for known desktops and servers, and conducting periodic configuration scans of desktops and laptops using the Nessus scanning tool. However, Kearney determined that the Corporation has not fully addressed prior vulnerability scanning and remediation weaknesses and new weaknesses were identified during the FY 2016 evaluation. Kearney observed multiple weaknesses with the management of the Corporation's vulnerability scanning and remediation process that impact the completeness and accuracy of vulnerability scan results. Specifically, Kearney identified continued vulnerability scanner configuration weaknesses and untimely remediation of server vulnerabilities. *Vulnerability Scanner Configuration Weaknesses* The Corporation and its MITS contractor did not appropriately configure the vulnerability scanning tool used to assess the Corporation's network for missing security patches and configuration errors. To ensure vulnerability scanning results are complete and accurate, organizations implement several key practices when conducting vulnerability scans. One fundamental practice is to confirm that the vulnerability scanner has valid credentials (i.e., user ID and password) and can successfully authenticate to targeted desktops, servers, and network devices. A second fundamental practice includes performing periodic network discovery scans to confirm that new servers or other network devices are included in weekly or monthly scans. Because passwords may change and new devices may be added to the Corporation's network, these practices are necessary to obtain complete and accurate vulnerability assessment results. Through observations of the Corporation's vulnerability scanner and discussions with knowledgeable IT staff from the MITS contractor, Kearney observed the following: 1. The Corporation and its MITS contractor lacked documented procedures (i.e., pre-scan checklist or post-scan checklist) for conducting weekly or monthly vulnerability scans of the Corporation's desktops, servers, and other network equipment.

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]

2. The Corporation and its MITS contractor configured the vulnerability scanner, Tenable Nessus, to scan by unique Internet Protocol (IP) address. While not inherently wrong, using an explicit list of static IP addresses, as opposed to domain names or IP ranges, does not ensure all devices will be scanned, as new virtual servers or other network equipment may be added to the network and accidently overlooked, or IP addresses may be changed.
3. The Corporation and its MITS contractor did not perform periodic (e.g., monthly or quarterly) network discovery scans to identify potentially new devices on the Corporation's network and update its static list of devices within Tenable Nessus. Further, the MITS contractor did not reconcile its Excel spreadsheet of static IP addresses against results from a discovery scan to identify new network devices or correct errors within the Excel spreadsheet.
4. The Corporation and its MITS contractor had never run Tenable Nessus' "Credential Scan Failure" report prior to August 30, 2016 to identify servers and other network devices that the Tenable Nessus scanner could not authenticate and evaluate. Further, the weekly review of vulnerability scan results did not identify that servers, located in the Demilitarized Zone (DMZ) network segment, experienced repeated authentication failures and needed further investigation. Examples of critical servers not scanned using credentials included a key network authentication server and the Oracle disaster recovery database servers, which contained copies of production data.
5. While the MITS contractor performed vulnerability scans of the operating system hosting the Corporation's eSPAN, eGrants, and MyAmeriCorps applications, the Corporation and its MITS contractor did not regularly scan the Oracle databases to identify database configuration errors and software vulnerabilities.
6. The MITS contractor advised Kearney that the password to the service account, used to scan the Corporation's Windows desktops and servers, had not been changed in the prior seven months.

Untimely Remediation of Server Vulnerabilities

Utilizing the available vulnerability scan information for the Corporation's servers as of August 28, 2016, Kearney prepared an aging analysis of the vulnerabilities present on the Corporation's servers. We calculated the age of a given vulnerability by comparing the vulnerability scan date (i.e., August 28, 2016) to the vulnerability check's publication date (i.e., Nessus's most recent plugin publication date) to approximate the age of vulnerabilities present on the Corporation's servers. Due to the limitations with the Corporation's vulnerability scanning process discussed above, ***Table 1: Aging of the Corporation's Server Vulnerabilities*** is an estimate based on the best available information as of August 28, 2016.

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]

Table 1: Aging of the Corporation's Server Vulnerabilities (as of August 28, 2016)

Risk Rating / (Unique Vulnerabilities)	<30 Days	31-90 Days	91-180 Days	181-365 Days	Over 365 Days	Grand Total
Critical (Unique)	77 (5)	6 (4)	20 (1)	90 (6)	0	**193** **(16)**
High (Unique)	239 (15)	43 (26)	134 (14)	155 (2)	198 (9)	**769** **(66)**
Medium (Unique)	106 (3)	127 (9)	85 (8)	235 (8)	339 (11)	**892** **(39)**
Low (Unique)	0	224 (3)	1 (1)	0	0	**225** **(4)**
Grand Total	**422**	**400**	**240**	**480**	**537**	**2,079**
Percentage	**20%**	**19%**	**12%**	**23%**	**26%**	**100%**
Total Unique Vulnerabilities	**23**	**42**	**24**	**16**	**20**	**125**

As ***Table 1*** highlights, 61%[29] of the detected server vulnerabilities are older than 90 days and trend upward, rather than downward, as time increases.

Lacking complete and accurate vulnerability scan results, the Corporation is unable to make informed decisions and prioritize resources to address security vulnerabilities. By not performing regular, authenticated vulnerability scans of the Corporation's databases, vulnerabilities may exist and remain unmitigated, thus increasing the likelihood that an external attacker could compromise the confidentiality, integrity, or availability of eSPAN, eGrants, or MyAmeriCorps portal. Collectively, incomplete vulnerability scan results understate the actual risks present in the Corporation's GSS.

Multiple factors have contributed to the weaknesses of the Corporation's vulnerability scanning and remediation processes since the issue was first reported as part of the FY 2014 FISMA evaluation. First, the Corporation and its MITS contractor have not prioritized the development of Standard Operating Procedures (SOP) for vulnerability scanning to address prior concerns raised during the FY 2014 and 2015 FISMA evaluations regarding the completeness and accuracy of vulnerability scan results. Second, as of September 1, 2016, the Corporation's Cybersecurity staff had not exercised sufficient oversight and review of the Tenable Nessus/Security Center configuration and vulnerability scanning practices to identify key omissions in its MITS contractor's practices. For example, the Corporation's Cybersecurity staff did not identify the need for periodic discovery scans or to investigate authentication failures. Since Kearney identified the vulnerability scanning weaknesses, the Corporation has initiated corrective actions, including performing authenticated scans of

[29] Sixty-one percent calculated as 12% + 23% + 26% for the periods 91-180 days, 181-365 days, and over 365 days.

<table>
<tr><th colspan="3">FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]</th></tr>
<tr><td colspan="3">database servers' operating system, and stated its intent to scan Oracle databases in the future. Regarding untimely remediation of identified vulnerabilities, the MITS contractor has not devoted sufficient resources to test and deploy security patches and/or configuration changes to resolve noted security vulnerabilities. Finally, the Corporation has not developed and established policy regarding the frequency that the password to service accounts must be changed.</td></tr>
<tr><td><b>FY 2014 Recommendations</b></td><td><b>FY 2015 Status</b></td><td><b>FY 2016 Status</b></td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #1: 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</td><td>In Progress</td><td>Closed</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #2: Include performance metrics for vulnerability management in future MDCS contracts</td><td>In Progress</td><td>Closed</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #3: 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</td><td>Closed</td><td>N/A</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #4: Test workstation performance during intrusive scans to determine the feasibility of obtaining comprehensive vulnerability scan results</td><td>Closed</td><td>N/A</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #5: Periodically perform scans of desktops and laptops using the current USGCB template from NIST to ensure ongoing compliance</td><td>In Progress</td><td>Closed</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #6: Upgrade or replace the Corporation's vulnerability scanning tool to overcome existing limitations and inaccurate scan results</td><td>In Progress</td><td>Closed</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #7: Implement a monthly process to review vulnerability scan configurations to include new vulnerability checks prior to scan execution</td><td>In Progress</td><td>Closed</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #8: Ensure that an appropriately configured vulnerability scan is conducted monthly against all information system components, including servers, routers, desktops, network printers, scanners, and copiers</td><td>In Progress</td><td>In Progress</td></tr>
<tr><td>FY 2014 – FISMA – NFR 2 – Rec #9: 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 (<i>Recommendation withdrawn and replaced with Recommendation FY 2016-FISMA-NFR-1-Rec #5)</i></td><td>In Progress</td><td>Closed</td></tr>
</table>

FY 2014 – FISMA – NFR 2: Multiple Weaknesses with Vulnerability Scanning and Remediation[23]
New FY 2016 Recommendations
FY 2016-Rec #1: Develop, document, and implement a vulnerability scanning process that incorporates periodic discovery scans, review and remediation of authentication failures, and periodic reconciliations to confirm that all known servers and network devices were scanned
FY 2016-Rec #2: Obtain technical training on the Corporation's vulnerability scanning solution to increase awareness of vulnerability scanning best practices and recommended configurations
FY 2016-Rec #3: Retain professional services from the software vendor or other independent expert to conduct an independent review of the Tenable Nessus installation and obtain recommendations for enhancing the vulnerability reporting solution
FY 2016-Rec #4: Require that the MITS contractor periodically change the password for privileged accounts (i.e., Domain Admin, root) used to conduct weekly vulnerability scanning
FY 2016-Rec #5: Perform authenticated vulnerability scans weekly of the critical Corporation applications and databases (eSPAN, eGrants, MyAmeriCorps portal)

FY 2014 – FISMA – NFR 3: Organizational Conflict of Interest[30]

NIST SP 800-53, Rev. 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 Federal Information Processing Standard (FIPS) Publication (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 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&M 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.

During the FY 2015 evaluation, 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 had 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 must be performed by an independent assessment team.

FY 2016 Update:

In the 2016 FISMA evaluation, the Corporation tasked the IAPS contractor with completing an independent security assessment of the GSS. The Corporation executed a delivery order for the IAPS contractor to serve as an independent third-party assessor for all Corporation systems and develop SA&A documentation. Kearney confirmed that the IAPS contractor followed the assessment process, delivered results to Corporation management in the SAR, and documented weaknesses in the GSS POA&M.

[30] For text of this prior-year finding, please refer to page 46 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. The full text of the original finding is available on page 27 of the published OIG Report Number 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 3: Organizational Conflict of Interest[30]		
FY 2014 Recommendations:	**FY 2015 Status**	**FY 2016 Status**
FY 2014 – FISMA – NFR 3 – Rec #1: 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	Closed
FY 2014 – FISMA – NFR 3 – Rec #2: Ensure that the 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	Closed
FY 2014 – FISMA – NFR 3 – Rec #3: Strengthen oversight of the organization’s IT contractors to ensure implementation of the SA&A process complies with Federal standards	In Progress	Closed

FY 2014 – FISMA – NFR 4: Use of an Obsolete and Unsupported Network Monitoring Tool[31]

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 of time (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 SOPs 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)[32] tool prior to the product's End-of-Life (EOL).

In FY 2015, the Corporation continued to use the obsolete Cisco MARS tool as the primary means for network monitoring and audit log analysis. Further, the new MITS contract did not contain a requirement to utilize hardware and software with vendor 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."

FY 2016 Update:

In the 2016 FISMA evaluation, Kearney noted that the Corporation has taken steps to resolve all of the six recommendations. The Corporation updated its standard security control language to require use of current, supported hardware and software. The MITS contractor replaced its network-monitoring tool, Cisco MARS, with a Security Information Event Management (SIEM) solution, Splunk, and implemented Tenable Security Center[33] and SolarWinds to supplement current network monitoring capabilities. With the proper configuration of Splunk, the Corporation is now capable of performing event and trend analysis to investigate security incidents with live data for up to 90 days and now archives

[31] For text of this prior-year finding, please refer to page 48 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For text of the original finding, please refer to page 30 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

[32] 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.

[33] The Corporation will require the network GSS contractor to use Nessus vulnerability scanner as part of the MITS contract.

FY 2014 – FISMA – NFR 4: Use of an Obsolete and Unsupported Network Monitoring Tool[31]

audit logs for at least one year. Further, Kearney noted the Corporation’s Symantec Backup Exec software retains network monitoring and audit data through 2013. The Corporation also took steps to strengthen oversight of the network monitoring and audit log process through periodic Operations meetings.

Weekly Operations and project status meeting were held to review the status of network monitoring and audit logging. During the April 13, 2016 meeting, the Corporation obtained evidence that all endpoints were configured to log Corporation events. The MITS contractor also performed an annual review and updated the audit and accountability procedures, which established the auditable events for the GSS.

To address other noted weaknesses, the Corporation released the second version of the Continuous Monitoring Strategy that defined the high-level metrics for security control process areas. For each monitoring area, the Corporation defined monitoring activities, the tools used for monitoring, and the frequency of monitoring. The Corporation also developed new SLAs with the MITS contractor, which included metrics such as the timely remediation of system vulnerabilities.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 4 – Rec #1: Identify and implement a replacement tool for network monitoring and audit log analysis to regain vendor software and hardware support	In Progress	Closed
FY 2014 – FISMA – NFR 4 – Rec #2: 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	Closed
FY 2014 – FISMA – NFR 4 – Rec #3: Ensure IT contracts include clauses requiring contractors to only utilize tools that have both software and hardware support (as applicable)	In Progress	Closed
FY 2014 – FISMA – NFR 4 – Rec #4: 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	Closed
FY 2014 – FISMA – NFR 4 – Rec #5: 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	Closed
FY 2014 – FISMA – NFR 4 – Rec #6: Develop and implement performance metrics to increase accountability for network monitoring and audit log review; improve effectiveness of	In Progress	Closed

FY 2014 – FISMA – NFR 4: Use of an Obsolete and Unsupported Network Monitoring Tool[31]		
information security; demonstrate compliance with Corporation policy, laws, and regulations; and identify areas for improvement		

FY 2014 – FISMA – NFR 6: Risks to the Confidentiality of Voice Communications[34]
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. Malicious individuals could exploit this 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.* During the 2015 evaluation, the Corporation 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.
FY 2016 Update: In the 2016 FISMA evaluation, the Corporation took steps to address prior-year recommendations. The Corporation initiated the process of restricting connectivity between the data virtual local area network (VLAN) and voice VLAN to only those devices that must communicate with both VLANs by implementing access control lists (ACL). The Corporation began by removing rules for the IP Communicator and began closing neutral ports used by the soft phones. The Corporation prepared and signed a Risk Acceptance Waiver in May of 2016. This waiver identified compensating controls and a corrective action plan (CAP) that was in the process of being implemented during the 2016 evaluation. Kearney noted that, subsequent to the conclusion of the FISMA evaluation, the Corporation plans to complete final corrective action tasks in December 2016. Through implementation of ACLs on routers, Kearney considers this recommendation to be closed. The Corporation conducted analysis to determine how the nine recommendations from NIST SP 800-58, *Security Considerations for Voice Over IP Systems*, would be implemented to improve the security over the Corporation's voice network. The Corporation also determined that the legacy Cisco desktop application was not needed, then it created a change request ticket to document removal from 24 desktops and laptops. Despite beginning the process, risks to the confidentiality of voice communications remain. Specifically, the Corporation added the prior-year recommendation to conduct penetration tests to the Corporate POA&M; however, IT contractors had not conducted a third-party assessment by the close of the FY 2016 FISMA evaluation. As a result, the Corporation may

[34] For text of this prior-year finding, please refer to page 51 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 36 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 6: Risks to the Confidentiality of Voice Communications[34]		
not be aware of the vulnerabilities in IT infrastructure (e.g., operating system, services, application) that an attacker may try to exploit. The Corporation does not plan to complete VoIP remediation plans until December 2016. As a result, the Corporation's LAN/WAN diagram and SSP did not accurately detail the implementation of actual VoIP solution and will require updates once corrective actions are completed.		
FY 2014 Recommendations	**FY 2015 Status**	**FY 2016 Status**
FY 2014 – FISMA – NFR 6 – Rec #1: Review the VoIP configuration and restrict connectivity between the Corporation's data VLAN and voice VLAN to only those devices that must communicate with both VLANs 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	Closed
FY 2014 – FISMA – NFR 6 – Rec #2: 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	Closed
FY 2014 – FISMA – NFR 6 – Rec #3: Consider contracting for a network penetration study and including the Corporation's voice network within the scope of the study	In Progress	In Progress
FY 2014 – FISMA – NFR 6 – Rec #4: 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	Closed
FY 2014 – FISMA – NFR 6 – Rec #5: Correct factual inaccuracies in the SSP for the LAN/WAN regarding the Corporation's VoIP infrastructure and identify compensating controls to address the risks associated with commingling data and VoIP networks	In Progress	In Progress

FY 2014 – FISMA – NFR 9: Inadequate Enterprise-Wide Risk Management Policies and Practices[35]

In 2014, Kearney reported that the Corporation documented its risk management policies and security controls in the Information Assurance Plan (IAP) and respective SSPs for its GSS and Major Applications (MA). However, these documents only described the risk management process at the information system (i.e., Tier 3)[36] level and discussed specific technical, management, and operational security controls focused at Tier 3. Existing risk management processes did not address risks at Tier 1: Organizational Perspective[37] and Tier 2: Mission/Business Process levels.[38] 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 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

During the 2015 FISMA evaluation, Kearney reported similar weaknesses associated with the Corporation's risk management process. The Corporation took some steps, but with limited

[35] For text of this prior-year finding, please refer to page 55 of the published Office of Inspector General (OIG) Report 16-03, Federal Information Security Modernization Act (FISMA) Evaluation of CNCS for FY 2015.
For the full text of the original finding, please refer to page 43 of the published OIG Report 15-03, Federal Information Security Management Act (FISMA) Independent Evaluation, for FY 2014.

[36] Tier 3 level 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 lifecycle (SDLC) process implemented across the organization.

[37] 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).

[38] 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 2014 – FISMA – NFR 9: Inadequate Enterprise-Wide Risk Management Policies and Practices[35]

progress, to resolve the prior-year weaknesses. The Corporation had documented the three tiers of management in the Enterprise Risk Management (ERM) 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 were held to make decisions concerning risks at the information systems level.

However, weaknesses remained 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 COOP needed 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 2016 Update:

During the 2016 FISMA evaluation, Kearney observed similar weaknesses associated with the Corporation's risk management process. Specifically, the Corporation's Chief Risk Officer (CRO) initiated a process to capture program risks through interviews with executives and staff. These organizational and program risks will be compiled into a risk register, which will be analyzed and prioritized by the Risk Management Council.

In addition, the Corporation began tracking Tier 1 organization-wide risks using the Corporation's POA&M. The risks currently tracked primarily included IT-specific weaknesses, such as prior-year recommendations on risk to the confidentiality and availability of voice communications (VoIP), weaknesses with the Corporation's security planning and assessment process, lack of adequate testing of the COOP, and inadequate controls over privacy.

Additionally, the Corporation's Capital Planning and Investment Board (CPIC) policy was updated to ensure that IT investments are aligned with business strategies, initiatives, and priorities. Likewise, the Corporation's Strategic Plan aligns goals with planned initiatives and the contractor resources and project plans committed towards those goals. As of September 2016, Kearney also noted the Risk Management Council met to identify risks to the Corporation and discuss remediation challenges. The Corporation also hired a new CRO to oversee the processes of the ERM program.

However, weaknesses remain with the Corporation's risk management and its policies and procedures. Specifically, the risk management process has not included steps to update the Corporation's POA&M to develop remediation plans and track organization-wide risks. In terms of tracking Tier 2 mission and business process risk, the Corporation did not provide evidence that they were tracking and developing remediation plans in a POA&M. Other issues with reporting in the Corporation's POA&M included inadequate documentation of

FY 2014 – FISMA – NFR 9: Inadequate Enterprise-Wide Risk Management Policies and Practices[35]

POA&M resource cost. Specifically, when the Corporation or contractors identified the resource required/level of effort, a numeric value or name of a person was provided, instead of quantifying the cost of resources required to remediate each failure or level of effort in human hours.

Additionally, the Corporation was in the process of developing a baseline understanding of risks to Tiers 1 and 2. Once the risk register is completed by the CRO and Risk Management Council, the Corporation can assign ownership and responsibilities, as well as understand the interconnections of tier risks to the Corporation's program risks.

Finally, the Corporation did not complete the process of addressing or capturing risk at the mission/business process levels. Specifically, the Corporation identified two Mission Essential Functions (MEF) that did not reflect the full scope of the Corporation's business processes. The Corporation plans to initiate the process of identifying the critical systems associated with MEFs, then determining the impact of loss, should an underlying IT system become unavailable during FY 2017.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 9 – Rec #1: Document and fully implement a comprehensive and enterprise-wide risk management process, including the following:	N/A	N/A
FY 2014 – FISMA – NFR 9 – Rec #1– Part 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	In Progress
FY 2014 – FISMA – NFR 9 – Rec #1– Part 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	In Progress
FY 2014 – FISMA – NFR 9 – Rec #1– Part 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	In Progress
FY 2014 – FISMA – NFR 9 – Rec #1– Part D: Integrating the risk management process with the CPIC process	In Progress	Closed

FY 2014 – FISMA – NFR 10: Weaknesses with the Corporation's Security Planning and Assessment Process[39]

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 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and 800-53, Rev. 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."

In 2015, the Corporation took steps to resolve the prior-year weaknesses by 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 SSPs, in particular, contained references to other documents, but the Corporation 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.

In FY 2015, the Corporation did not address 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. Further, the Corporation still had 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 assessing 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."

FY 2016 Update:

In the 2016 FISMA evaluation, Kearney noted that the Corporation took steps to strengthen the security assessment process. In the process, the Corporation closed seven of 13 open

[39] For text of this prior-year finding, please refer to page 57 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 48 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation, for FY 2014.*

FY 2014 – FISMA – NFR 10: Weaknesses with the Corporation's Security Planning and Assessment Process[39]

prior-year recommendations. The Corporation's Cybersecurity Policy 376 *Cybersecurity Policy* and Cybersecurity Control Families Document (CFD) establish the control policy and organization-defined parameters for information systems. Where the CFD identifies the Corporation as the control owner, it documents common controls based on NIST SP 800-53, Rev. 4 and defines required implementation parameters. The CFD also establishes the requirement for privacy control ownership and documents whether the Corporation or IT contractors must implement system-specific controls and privacy controls.

The Corporation also published the Risk Management Framework (RMF) Guide in FY 2016 to establish a single security assessment process consistent with NIST SP 800-37, Rev. 1 and NIST SP 800-53A for the Corporation's IT vendors to use. The contents within the RMF Guide prescribe a six-step process, identify the responsibilities of the security control assessor, and required security documentation that must be generated by an independent security control assessor as an outcome of the security assessment process. The RMF Guide also establishes the policy requirement that an independent party must perform assessments.

Additionally, the Corporation updated SSPs to include an implementation statement and identified the party who was responsible for implementing and maintaining each NIST SP 800-53 control, excluding privacy controls.

Finally, the Corporation developed a plan to track progress on implementing privacy controls and documented results in the Corporation's CFD for the NIST privacy controls. For each control, the Corporation specified whether it was implemented; whether it applies to the organization, network, or application level; and how the Corporation planned to address the control.

However, the Corporation has not completely implemented the recommendations to improve the Corporation's security planning and assessment process. While the Corporation's RMF Guide establishes clear expectations describing how the security assessment process must be conducted, the Corporation's security assessment standards do not address recommendations to create a sampling plan or develop standard control test cases or questionnaires to promote repeatability and consistency.

Though the Corporation took steps in the CFD to assign responsibility for implementing specific NIST SP 800-53 security and privacy controls to either Corporation or the IT contractor, the Corporation does not have the ability to compel contractors to comply with these responsibilities. This is due to the Corporation's decision not to update existing contracts to include required security language due to resource constraints.

The Corporation established expectations for ownership of privacy controls based upon the Privacy Plan and CFD, where control ownership responsibilities fall upon both the Corporation and an IT contractor.

FY 2014 – FISMA – NFR 10: Weaknesses with the Corporation's Security Planning and Assessment Process[39]

At the close of the FY 2016 FISMA evaluation in September 2016, the Corporation was planning the annual assessment of eSPAN and Momentum, but it did not have any completed test results. Kearney confirmed that the Corporation's IAPS completed the assessment of the GSS in 2016 and produced SAR and POA&M documentation. Without a completed security assessment of all systems, the Corporation may not be aware of the security risks present on its systems.

In the Privacy Controls Implementation Plan, dated July 31, 2015, the Corporation documented that privacy controls were implemented; however, further research revealed that several privacy controls from Appendix J of NIST SP 800-53, Rev. 4 were "planned" rather than "implemented." Specifically, Kearney noted DM-1 *Minimization of Personally Identifiable Information*, SE-2 *Privacy Incident Response*, and TR-1 *Privacy Notices* are planned controls.

Finally, the Authorizations to Operation (ATO) for GSS, Momentum, and eSPAN were not annually re-authorized as required by OMB and NIST SP 800-53, Rev. 4 CA-7 Continuous Authorizations. Specifically, the GSS ATO was last signed by the CIO on May 24, 2013; the Momentum ATO was last signed by Chief Operating Officer (COO) on October 8, 2014; and the eSPAN ATO was last signed by the Information System Owner (ISO) on November 21, 2013. During the FY 2016 FISMA evaluation, the Corporation had not completed an annual review of security controls for all systems, but it had completed the annual test of the GSS.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 10 – Rec #1: Develop and implement a single security assessment process consistent with NIST SP 800-37, Rev. 1, and NIST SP 800-53A for the Corporation's IT vendors to utilize	In Progress	Closed
FY 2014 – FISMA – NFR 10 – Rec #2: Establish security assessment standards, to ensure consistency and quality, such as:	N/A	N/A
FY 2014 – FISMA – NFR 10 – Rec #2– Part A: Sampling plan	In Progress	In Progress
FY 2014 – FISMA – NFR 10 – Rec #2– Part B: Standard test cases	In Progress	In Progress
FY 2014 – FISMA – NFR 10 – Rec #2– Part C: Determination of security assessor independence requirements	In Progress	Closed
FY 2014 – FISMA – NFR 10 – Rec #3: Review all NIST SP 800-53, Rev. 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	Closed
FY 2014 – FISMA – NFR 10 – Rec #4: 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.	In Progress	Closed

FY 2014 – FISMA – NFR 10: Weaknesses with the Corporation’s Security Planning and Assessment Process[39]		
Incorporate the results of such analysis in the resulting IT contract to avoid ambiguity and subsequent vendor requests for a change order		
FY 2014 – FISMA – NFR 10 – Rec #4: Create a “Common Controls” security plan and privacy controls security plan for the security controls for which the Corporation will retain responsibility	In Progress	Closed
FY 2014 – FISMA – NFR 10 – Rec #5: Update the SSPs for eSPAN, Momentum, and LAN/WAN to ensure:	N/A	N/A
FY 2014 – FISMA – NFR 10 – Rec #5– Part A: SSP contains an accurate description of the information system and any sub-systems	Closed	N/A
FY 2014 – FISMA – NFR 10 – Rec #5– Part B: SSP clearly identifies the information system boundaries and technologies utilized within the boundary	Closed	N/A
FY 2014 – FISMA – NFR 10 – Rec #5– Part C: Responsibility for implementing each NIST SP 800-53 control is clearly delineated between the Corporation and IT vendor	In Progress	In Process
FY 2014 – FISMA – NFR 10 – Rec #5– Part D: SSPs accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls and required control enhancements	In Progress	In Progress
FY 2014 – FISMA – NFR 10 – Rec #6: 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	Closed
FY 2014 – FISMA – NFR 10 – Rec #7: 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	In Progress
FY 2014 – FISMA – NFR 10 – Rec #8: Annually assess a subset of the Corporation’s common controls and privacy controls	In Progress	In Progress
FY 2014 – FISMA – NFR 10 – Rec #9: 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 forms in a central location so they may be readily searched during risk considerations	In Progress	Closed

FY 2014 – FISMA – NFR 11: Lack of Formal Role-Based Training[40]

In FY 2014, the Corporation had 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 several NIST SPs, including 800-16 and 800-53, Rev. 4. Kearney first reported this issue in 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 or targeted for different individual job functions. This awareness training did not meet the requirements of NIST SP 800-53, Rev. 4, AT-3 *Role-Based Security Training* 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."

During FY 2014, IT contractors for the Corporation's two major applications, Momentum and eSPAN, received no additional training beyond the general information security awareness training offered by the Corporation. In addition, the Corporation provided limited evidence of role-based training for certain individuals with significant information security responsibilities.

In the FY 2015 FISMA evaluation, Kearney reported similar weaknesses associated with the Corporation's security training process. The Corporation 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, which was utilized originally in FY 2014 and then again in FY 2015. Similar to FY 2014, IT contractors for the Corporation's two major applications received no training beyond what was offered by the Corporation. In addition, the Corporation provided limited evidence of role-based training for certain individuals with significant information security responsibilities.

The Corporation's prior IT contracts and the new contract, MITS,[41] did not specifically require that IT contractors provide role-based security training for its employees serving the Corporation. For example, software developers were not required to complete any specific training on developing secure software. In FY 2015, the Corporation had not required its IT vendors to demonstrate that employees serving the Corporation had completed annual

[40] For text of this prior-year finding, please refer to page 60 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 56 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

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

FY 2014 – FISMA – NFR 11: Lack of Formal Role-Based Training[40]

specialized training. 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.

FY 2016 Update:

During the 2016 FISMA evaluation, the Corporation implemented all three recommendations to ensure role-based training was developed and taken by the Corporation and its IT contractors. Specifically, the Corporation created role-based training and instituted a process to collect evidence of security training completion for the Corporation’s employees and IT contractors with significant information security responsibilities. Specifically, the Corporation developed role-based training tailored for Authorizing Officials (AO), ISOs, Information System Security Managers (ISSM), and ISSOs. Additionally, the Corporation maintained a record of individuals who attended training including contractors.

The Corporation’s updated SOW with the MITS contractor included requirements that compel the contractor to meet security requirements of the agency. Finally, the Corporation collected evidence from employees and IT contractors, and stored records on an internal SharePoint site.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 11 – Rec #1: 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	Closed
FY 2014 – FISMA – NFR 11 – Rec #2: 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	Closed
FY 2014 – FISMA – NFR 11 – Rec #3: Maintain evidence of security training for the Corporation’s employees and IT contractors with significant information security responsibilities	In Progress	Closed

FY 2014 – FISMA – NFR 12: Improvements Needed to POA&M Reporting[42]

In the FY 2014 FISMA evaluation, the Corporation did not have an adequate POA&M management process in place to ensure that all known security weaknesses were recorded, resources needed for remediation were identified, and progress toward timely resolution was 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 OMB guidance and NIST SPs, including 800-65 *Integrating IT Security into the Capital Planning and Investment Control Process*, and 800-53, Rev. 4, *Recommended Security Controls for Federal Information Systems and Organizations*.

During the FY 2015 FISMA evaluation, Kearney reported similar weaknesses associated with identifying required resources with the Corporation's POA&M management process. The Corporation took 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, implemented quarterly POA&M reviews, and established a new POA&M format. The Corporation prepared a draft SOP for POA&M management, which is designed to assist ISSOs/ISSMs, ISOs, and supporting OIT staff in identifying, assessing, prioritizing, monitoring, and routinely reporting on the progress of corrective actions taken to remediate security weaknesses. In addition, the Corporation issued a POA&M policy document detailing guidance and reporting requirements to all system owners. The CIO reported that the Corporation was better able to hold ISOs 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 item.

However in FY 2015, weaknesses related to the Corporation's POA&M process remained. 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 POA&Ms, which included missing resources (i.e., technical or work hours), estimated resolution costs, and milestone completion dates.

[42] For text of this prior-year finding, please refer to page 62 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 60 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 12: Improvements Needed to POA&M Reporting[42]

FY 2016 Update:

During the FY 2016 FISMA evaluation, the Corporation implemented the three prior-year recommendations to improve the Corporation's POA&M management process. The Corporation finalized its SOP for POA&M management on October 17, 2015 and updated it on April 20, 2016.

Kearney tested the risk acceptance process and found the Corporation developed Risk Acceptance Waivers for known vulnerabilities. Corrective Action Plans (CAP) and compensating controls were identified and added to waivers, then signed by management to grant a temporary approval to operate under the accepted risks.

The Corporation's CISO conducted weekly meetings to review POA&M lists managed by the Corporation and IT contractors. These POA&M meetings escalated issues to OIT and also provided the ability to ensure all POA&Ms met the quality standards established by the Corporation.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 12 – Rec #1: Enhance the POA&M process to identify resources required for remediation in either the POA&M item or associated change request ticket	In Progress	Closed
FY 2014 – FISMA – NFR 12 – Rec #3: Document acceptance of risk for items that will not be remediated, along with planned mitigating controls	In Progress	Closed
FY 2014 – FISMA – NFR 12 – Rec #4: 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 COO on known security weaknesses and associated resource needs to coincide with budget requests	In Progress	Closed

FY 2014 – FISMA – NFR 13: Inadequate Controls Over Remote Access[43]

Corporation-issued laptops were configured to connect automatically to the Corporation's network through 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 FIPS 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 800-52, Rev. 1, *Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations*.

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.

At the close of the FY 2015 FISMA evaluation, 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.

In the FY 2015 evaluation, the Corporation made limited progress to resolve the prior-year weaknesses, but it planned to include Personal Identity Verification (PIV) card implementation in the FY 2017 budget.

FY 2016 Update:

During the FY 2016 FISMA evaluation, the Corporation addressed two of the three prior-year recommendations to strengthen controls over remote access. The Corporation's CISO, CIO, and Chief Risk Officer (CRO) signed a Risk Acceptance Waiver in July 2016 to acknowledge and accept the risk that the Corporation has not deployed PIV cards for logical access to the Corporation's laptops and for remote access to the Corporation's network. The Corporation has requested funding of $100,000 to implement PIV authentication in the FY 2017 IT budget. The Corporation is tracking a POA&M for the MITS contractor to purchase VPN hardware capable of supporting a FIPS-compliant encryption protocol (TLSv1.2 or greater) with the scheduled completion date in December 2016. The Corporation tracked remediation activities occurred through Operations meetings between OIT and the Corporation's MITS contractor. The failure to timely remediate the known vulnerability leaves remote network traffic open to the risk of compromise, potentially leading to a breach of PII or other sensitive data.

[43] For text of this prior-year finding, please refer to page 64 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 63 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 13: Inadequate Controls Over Remote Access[43]		
FY 2014 Recommendations	**FY 2015 Status**	**FY 2016 Status**
FY 2014 – FISMA – NFR 13 – Rec #1: 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	In Progress
FY 2014 – FISMA – NFR 13 – Rec #2: Implement a VPN solution that complies with OMB Memorandum M-06-16 and NIST SP 800-53, Rev. 4, mandatory security controls for Federal agencies by using multi-factor authentication where one factor is separate from the device gaining access	In Progress	Closed
FY 2014 – FISMA – NFR 13 – Rec #3: Strengthen oversight of MDCS contractors (now MITS contractor) 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	Closed

FY 2014 – FISMA – NFR 14: Inadequate DRP Documentation and Planning[44]

In FY 2014, the Corporation's DRP did 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, address all essential business functions. Further, the Corporation's DRP was written specifically for the MDCS contractor; 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.

During the 2015 assessment, 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 to a lack of testing, the Corporation did not conduct a BIA to identify organizational risks that should be addressed in the Continuity of Operations Plan (COOP), nor did it develop an agency-wide COOP, a GSS DRP, and a financial system Contingency Plan. The Corporation provided Kearney with a draft COOP; however, the Corporation did not follow guidance per NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*, which states the "COOP should not be completed without a completed BIA."

FY 2016 Update:

During the FY 2016 FISMA evaluation, the Corporation made limited progress to resolve weaknesses associated with the Corporation's Disaster Recovery Plan (DRP) documentation and planning. Prior-year recommendations noted the lack of congruency between the Corporation's system BIAs and the business and mission functions that are essential for the continuity of operations. During the 2016 FISMA evaluation, the Corporation established two Mission Essential Functions (MEF):

1. MEF #1 – Ensure the safety and welfare of AmeriCorps National Civilian Community Corps (NCCC) members serving at five campus locations throughout the United States
2. MEF #2 – Activate the Disaster Services Unit (DSU).

However, the Corporation mistakenly completed BIA documentation for these two MEFs and created new BIA documentation aligned with FEMA guidance instead of NIST SP 800-34,

[44] For text of this prior-year finding, please refer to page 66 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 67 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation* for FY 2014.

FY 2014 – FISMA – NFR 14: Inadequate DRP Documentation and Planning[44]

Rev. 1, *Contingency Planning Guide for Federal Information Systems,* Appendix B. As a result, the contents of the two MEF BIAs are not consistent with requirements and format found in NIST SP 800-34, Rev. 1. Specifically, the BIAs do not identify MEFs related to the Corporation’s strategic goals, nor do they document critical business processes and their reliance on IT systems. The BIAs do not establish Recovery Time Objectives (RTO), Recovery Point Objectives (RPO) or identify and prioritize the information systems associated with supporting the MEFs. Likewise, the current and former BIA documentation does not identity infrastructure that supports these information systems and does not reflect the Corporation’s current assessment.

During the FY 2016 evaluation, the Corporation indicated that it was in the process of identifying the information systems associated with the two MEFS. The Corporation noted that the process planned for FY 2017 will ultimately lead to a determination of recovery criticality for information systems required to maintain MEFs and possibly identify new MEFs.

The Corporation also activated their DRP in response to an unplanned Ransomware event that encrypted a large number of files stored on a shared network drive. In response to the event, the Corporation restored these encrypted files over a period of four days. The Corporation also participated in a continuity of operations exercise, which brought management’s attention to deficiencies in COOP documentation that prevented the Corporation from exercising the plan during the exercise. At the close of FISMA testing, the Corporation had not finalized its COOP.

Kearney noted that the Corporation still 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. Lastly, there is no contractual requirement for annual DRP testing in the new MITS contract and for the MITS contractor to restore critical systems at the alternate site.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 14 – Rec #1: Kearney recommends that the Corporation develop a more effective and comprehensive DRP and COOP by:	N/A	N/A
FY 2014 – FISMA – NFR 14 – Rec #1 – Part A: Developing an individual BIA for each critical system with participation from the business owner based upon the BIA template format found in NIST SP 800-34, Rev. 1	In Progress	In Progress
FY 2014 – FISMA – NFR 14 – Rec #1 – Part B: Determining information system recovery criticality, including allowable downtime and acceptable data loss based on business process needs	In Progress	In Progress

FY 2014 – FISMA – NFR 14: Inadequate DRP Documentation and Planning[44]		
FY 2014 – FISMA – NFR 14 – Rec #1 – Part C: Identifying outage impacts, resource requirements, and recovery priority for system resources	In Progress	In Progress
FY 2014 – FISMA – NFR 14 – Rec #1 – Part D: Updating the DRP to cover the entire Corporation and other critical IT contractors and not just the MITS contractor	In Progress	In Progress
FY 2014 – FISMA – NFR 14 – Rec #1 – Part E: Updating the COOP based on revisions to the BIA and DRP	In Progress	In Progress

FY 2014 – FISMA – NFR 15: Lack of Adequate Testing of Continuity of Operations Plan[45]

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 MEFs 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 MEFs and the agency's financial system, did not exist.

The Corporation did not follow NIST SP 800-34, Rev. 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."

In FY 2015, 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 did it develop an agency-wide COOP, a GSS DRP, and a financial system Contingency Plan. The Corporation provided a draft COOP; however, the draft documents suggested the Corporation did not follow guidance per NIST SP 800-34, Rev. 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 in FY 2015.

In addition, the responsibility for the COOP was assigned to the COOP Executive Team (CET), placing control under the purview of multiple individuals, as opposed to a single 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.

Subsequent to the completion of Kearney's fieldwork in August 2015, the Corporation reported that it was in the process of identifying the stakeholders for mission/business

[45] For text of this prior-year finding, please refer to page 67 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 70 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 15: Lack of Adequate Testing of Continuity of Operations Plan[45]

functions enterprise-wide to complete the BIA and update the COOP and DRP. This effort would also enable documentation of MEFs, 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 planned to implement and document the annual COOP exercise, as well as share the lessons learned from these exercises.

FY 2016 Update:

During the FY 2016 evaluation, the Corporation implemented all four of the prior-year recommendations to strengthen continuity of operations planning and testing. Specifically, the Corporation made updates to the COOP to align the plan with two new MEFs included.

Additionally, the Corporation updated the COOP and designated a COOP Coordinator response for facilitating communication among COOP stakeholders. The COOP also defined a clear chain of command of personnel overseeing essential functions.

Finally, the Corporation made progress to resolve weaknesses associated with the Corporation's COOP planning and testing. The Corporation exercised its ability to respond and recover operations from unplanned events that occurred in FY 2016. Specifically, the Corporation also instructed its employees to work remotely and access the Corporation's network, systems, and resources during the Pope's visit and a major snowstorm. The Corporation also activated their COOP and DRP in response to an unplanned Ransomware event that encrypted a large number of files stored on a shared network drive. In response to the event, the Corporation restored these encrypted files over a period of four days. These unplanned events demonstrated that the Corporation has the ability to sustain operations due to short-term impacts of three to five days.

FY 2014 Recommendations	FY 2015 Status	FY 2016 Status
FY 2014 – FISMA – NFR 15 – Rec #1: Define a clear chain of command to clarify responsibilities and identify an Information System Contingency Plan (ISCP) Director to oversee Corporation-essential functions regarding the COOP	In Progress	Closed
FY 2014 – FISMA – NFR 15 – Rec #2: Review the assumptions that are included in COOP documentation and ensure that the assumptions are valid and realistic	In Progress	Closed
FY 2014 – FISMA – NFR 15 – Rec #3: Update the COOP documentation to ensure that all MEFs are considered and have detailed plans for resumption of operations	In Progress	Closed
FY 2014 – FISMA – NFR 15 – Rec #4: Conduct a COOP test at least annually and capture lessons learned in a formal after-action report	In Progress	Closed

FY 2014 – FISMA – NFR 16: Inadequate Controls over Privacy Data[46]

At the close of the 2014 FISMA evaluation, the Corporation had not explicitly documented its privacy controls, as required by NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J: "Privacy Controls." 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.

Further, the Corporation had not updated and publicly posted the PIAs for two key information systems, Momentum or eSPAN, since 2009.

In the FY 2015 FISMA evaluation, the Corporation prepared an initial version of its Privacy Controls Implementation Plan (Appendix J of NIST SP 800-53, Rev. 4) 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 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 PIAs 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 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 of 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 (HQ). Specifically, two boxes of mail were found at the Corporation's headquarters unattended in the front hallway at the United Stated Postal Service (USPS) mailbox, which included program members' address and other PII visible through the envelopes' address windows. As individuals continue to retain records containing PII beyond the statutory period or fail to secure PII information properly, Kearney concluded that the

[46] For text of this prior-year finding, please refer to page 69 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015. For full text of the original finding, please refer to page 73 of the published OIG Report 15-03, *Federal Information Security Management Act (FISMA) Independent Evaluation*, for FY 2014.

FY 2014 – FISMA – NFR 16: Inadequate Controls over Privacy Data[46]

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.

FY 2016 Update:

During the 2016 FISMA evaluation, Kearney noted that the Corporation implemented all seven prior-year recommendations to enhance controls over privacy data. Specifically, the Corporation initiated a new process to collect and document an inventory of PII within information systems at HQ and remote NCCC and state offices. The Corporation's system inventory was consistent with information collected from PIA answers from the network GSS, eSPAN, Momentum, VISTA Healthcare Benefits (VHB), and NCCCs and included the quantity of PII, sensitivity and type of PII, PIA status, confidentiality impact, whether PII is shared, who has access, and how long it is retained. The Corporation confirmed the location of PII and controls over PII at Corporation sites using a security questionnaire. Additionally, the Corporation tracked PII stored at HQ using a list and within FISMA information systems. The physical PII inventory included the point of contact (POC) name, record description, and specific storage location (e.g., file cabinet or room number).

As part of our procedures to evaluate the Corporation's implementation of privacy controls, Kearney performed site visits at the AmeriCorps Pacific NCCC Campus and Seattle, WA state office. We observed that NCCC complied with requirements for destroying outdated records containing PII. Kearney inspected locations used to store PII and noted files were stored based on year and then shredded. We also noted during the site visit to the Seattle, WA state office that files with PII were stored in a locked cabinet and the site used a crosscut shredder to destroy outdated records in accordance with NARA.

Kearney noted that the Corporation took part in National Data Privacy Day on January 28, 2016 to educate employees on the importance of protecting PII. The Corporation sent out e-mails detailing different ways employees could protect personal information and provided links to more in-depth information on the topics. This event, combined with annual role-based security training, offered employees sufficient training on how to manage and protect PII.

Kearney obtained the most recent PIAs for both eSPAN and Momentum to determine when the PIAs were last updated or reassessed. We noted that the eSPAN PIA was assessed and signed on June 7, 2016, and the Momentum PIA was signed by management on July 8, 2016.

The Corporation CIO remains the Senior Agency Official for Privacy (SAOP)/CPO and the Cybersecurity Team supports the CIO with the implementation of privacy controls. During FY 2016, the Corporation approved a Privacy Controls Implementation Plan that documents the organizational controls for protecting privacy and PII within Corporation systems and documented privacy control requirement ownership between the Corporation and contractors in the CFD.

FY 2014 – FISMA – NFR 16: Inadequate Controls over Privacy Data[46]		
FY 2014 Recommendations	**FY 2015 Status**	**FY 2016 Status**
FY 2014 – FISMA – NFR 16 – Rec #1: Update, document, and implement the privacy controls required by Appendix J of NIST SP-800-53, Rev. 4 and perform continuous monitoring, as necessary, to comply with the provisions of the publication	In Progress	Closed
FY 2014 – FISMA – NFR 16 – Rec #2: 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	Closed
FY 2014 – FISMA – NFR 16 – Rec #3: 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	Closed
FY 2014 – FISMA – NFR 16 – Rec #4: Ensure Corporation staff are aware of, and comply with, NARA retention requirements for maintaining physical PII records	In Progress	Closed
FY 2014 – FISMA – NFR 16 – Rec #5: 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	Closed
FY 2015 New Recommendations		
FY 2015 – FISMA – NFR 1 – Rec #1: Designate a CPO to ensure an individual is identified and assigned responsibility for privacy controls	New	Closed
FY 2015 – FISMA – NFR 1 – Rec #2: Enhance security training for all employees to address awareness of PII and records management security	New	Closed

FY 2015 – FISMA – NFR 1: Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses [47]

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/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.

The Corporation received only two proposals for the seven-year IT services BPA worth potentially $50 million. According to the Office of Procurement Services (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.

Two serious flaws compromised the award of the replacement contract, by which the Corporation intended to remediate 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 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.

[47] For text of this prior-year finding, please refer to page 21 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015.

FY 2015 – FISMA – NFR 1: Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses [47]

Without Contractor Performance Assessment Reporting System (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.

FY 2016 Update:

During the FY 2016 FISMA evaluation, the Corporation implemented all six prior-year recommendations to prevent future IT contract delays. Specifically, the Corporation created a new version of IT security language to be incorporate into new or revised IT contracts. The Corporation also documented a process to ensure that Office of Procurement Services (OPS) incorporates required security language into future IT contracts. In coordination with the documented procurement business processes, the Corporation held training to communicate with Contracting Officer's Representatives (COR) a requirement to complete CPARS evaluations upon completion of all contracts over $150,000.

In order to increase the Corporation's leverage to compel IT contractors to meet IT security requirements, the Corporation incorporated updated security contract language and requirements in the current task order for the MITS contractor based upon the Corporation's latest security language. In conjunction with the updated task order, the Corporation developed new SLAs to better measure the performance and adherence to the security requirements. Examples of performance metrics include timelines to remediate known vulnerabilities, captured in MITS SLA #19 of 20.

The Corporation implemented a monthly project report to gauge how well the MITS contractor delivered services. The Corporation measured the contractor's performance in 19 areas, including the resources provided to the Corporation, how well budget was used, adequate implementation of technical solutions, and on-time and in-scope delivery.

FY 2015 Recommendations	FY 2016 Status
FY 2015 – FISMA – NFR 1 – Rec #1: Update the Corporation's standard information security language for contracts to include measures of performance	Closed
FY 2015 – FISMA – NFR 1 – Rec #2: Develop SLAs and measures of performance and incorporate such into the MITS contract	Closed
FY 2015 – FISMA – NFR 1 – Rec #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	Closed
FY 2015 – FISMA – NFR 1 – Rec #4: Develop and deliver training for customers of OPS on SOW development and include instructions on completing the Source Selection Determination Memorandum	Closed
FY 2015 – FISMA – NFR 1 – Rec #5: Require CORs to complete CPARS evaluations upon completion of all contracts over $150,000	Closed

FY 2015 – FISMA – NFR 1: Inadequate Planning and Untimely Award of Information Technology Contract Delays Remediation of Information Security Weaknesses [47]	
FY 2015 – FISMA – NFR 1 – Rec #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 Statement of Work (SOW) and requesting industry comments, and contacting potential bidders to gauge their willingness to bid, ensuring sufficient competition for an award	Closed

FY 2015 – FISMA – NFR 2: Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement [48]

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.

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.

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 with their current job functions.

FY 2016 Update:

During the FY 2016 FISMA evaluation, Kearney identified similar control weaknesses found in prior years. These included untimely deactivation and removal of GSS and Momentum accounts due to reliance upon manual processes.

[48] For text of this prior-year finding, please refer to page 27 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015.

FY 2015 – FISMA – NFR 2: Access Controls over the Corporation's Network and Momentum Financial User Accounts Need Improvement [48]

The 2016 FISMA evaluation concluded that manual access control processes still exist at the Corporation. The Corporation's security administrators (SA) follow a process to manually disable inactive accounts when notified through a script that runs on a bi-monthly basis. For those users whose accounts were not disabled, the Corporation created Risk Acceptance Waivers until users returned from extended leave.

Continued management attention is required to enhance access controls over the Corporation's network and Momentum user accounts. Specifically, the Corporation's MITS contractor's "inactivity script" did not identify and disable GSS accounts that meet inactivity requirements of 30 days. Kearney's testing confirmed that several accounts were not timely disabled due to the flawed design of the script, which ran bi-monthly rather than daily. This design flaw has the potential to leave an inactive account unlocked for up to 45 days.

The Corporation's manual account review process also failed to delete "disabled" accounts after 30 days. Specifically, during the Corporation's Momentum account review process that occurred on April 30, 2016, two of 18 accounts had a last logon date from October 2015, three last logged in November 2015, and three last logged on in December 2015.

As a result of not redesigning account review processes to automatically alert the Corporation to disable inactive GSS and Momentum user accounts on a daily basis, user accounts may be accessed and utilized by an unauthorized individual to commit acts of fraud or abuse, increasing the risk that the integrity and confidentiality of Corporation's data are manipulated or leaked by an unauthorized individual.

FY 2015 Recommendations	FY 2016 Status
FY 2015 – FISMA – NFR 2 – Rec #1: 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	In Progress
FY 2015 – FISMA – NFR 2 – Rec #2: Implement an automated alert to notify the Corporation on a daily basis when accounts "disabled" after 30 days must be deleted. 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 OU that is not subject to automatic deletion (modified repeated condition from FY 2015)	In Progress
FY 2015 – FISMA – NFR 2 – Rec #3: Require SAs to disable accounts timely after completion of the quarterly account review process unless they receive confirmation that user access remains appropriate	Closed

FY 2015 – FISMA – NFR 3: Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan [49]

During the FY 2015 FISMA evaluation, Kearney noted that the Corporation's current IT Strategic Plan was last updated in FY 2013 and did not reflect current IT modernization efforts. The plan did not describe the Corporation's long-term goals and strategies for leveraging IT to satisfy business needs. Additionally, the IT Strategic Plan did 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 Enterprise Architecture Plan (EAP).

The CIO informed Kearney that the Corporation intends to implement cloud-based computing 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 cloud service provider offers 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.

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. 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.

FY 2016 Update:

During the 2016 FISMA evaluation, the Corporation took significant steps to implement all of the six prior-year recommendations. Specifically, the Corporation updated the IT Strategic Plan and create an Enterprise Architecture Plan (EAP) by implementing four of the six recommendations. The Corporation's IT Strategic Plan, published on February 22, 2016, organized OIT's activities with four strategic goals. For example, Strategic Goal #2 addresses the modernization of technology and services, specifically stating its objectives as: 1) modernize grants and member management application; 2) enhance records management, internal and external information sharing, and collaboration; and 3) implement flexible, cost-effective, data-driven IT services to enable business agility and productivity, as well as enhance user experience. Using the new IT Strategic Plan, the Corporation is prepared to better align project plans, personnel, and deliverables with one of the strategic goals.

[49] For text of this prior-year finding, please refer to page 31 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015.

FY 2015 – FISMA – NFR 3: Outdated Information Technology Strategic Plan and Lack of Enterprise Architecture Plan [49]

The Corporation's initial version of the EAP was published on May 24, 2016. The EAP currently includes an outline of the enterprise architecture's purpose, principles, and framework. Management controls, the Corporation's core products and services, target solutions, technologies, and security requirements are described in relation to the Corporation's architecture.

The Corporation defined continuous monitoring metrics within the ISCM strategy and also developed IT measures of performance in new MITS SLAs. Specifically, SLA-19 documents requirements to remediate critical vulnerabilities based upon the Corporation's remediation timelines and includes instructions in the event a requirement cannot be met.

The Corporation also developed a project portfolio that provides organization of IT projects that are aligned with the IT Strategic Plan. Within each project, the Corporation created a Microsoft SharePoint site to record the project activities, risks, and deliverables. Each project is required to create formal a project plan in Microsoft Project, where tasks are assigned to resources, including project personnel, resources, and contractors.

FY 2015 Recommendations	FY 2016 Status
FY 2015 – FISMA – NFR 3 – Rec #1: Immediately update its IT Strategic Plan by:	N/A
FY 2015 – FISMA – NFR 3 – Rec #1 – Part A: Including current IT modernization efforts and future IT investments	Closed
FY 2015 – FISMA – NFR 3 – Rec #1 – Part B: Updating performance metrics to measure success and determine if milestones are being reached	Closed
FY 2015 – FISMA – NFR 3 – Rec #1 – Part C: Defining roles and responsibilities of identified human resources	Closed
FY 2015 – FISMA – NFR 3 – Rec #1 – Part D: Periodically updating the Strategic Plan to reflect major changes in IT strategy	Closed
FY 2015 – FISMA – NFR 3 – Rec #2: Immediately develop an EAP by:	N/A
FY 2015 – FISMA – NFR 3 – Rec #2 – Part A: Highlighting the target solutions, technologies, and security requirements	Closed
FY 2015 – FISMA – NFR 3 – Rec #2 – Part B: Periodically updating the EAP to mirror any changes and remain in sync with the IT Strategic Plan	Closed

FY 2015 – FISMA – NFR 4: Inaccurate Inventory of Physical IT Asset [50]

On July 30, 2015, Kearney visited the Philadelphia FFMC and the Pennsylvania state office. The following day, Kearney visited the Baltimore 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 HQ, 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
- An external two (2) Terabyte (TB) Passport External Hard Drive was not recorded on the inventory list.

FFMC

- Three IT assets were not recorded on the IT inventory list.

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.

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.

FY 2016 Update:

During the 2016 FISMA evaluation, the Corporation took steps to implement three out of four of the prior-year recommendations to correct the inaccurate inventory of physical IT assets. Specifically, the Corporation implemented an automated system to track IT assets and chose to maintain a separate system to maintain other physical inventory assets. The Corporation also communicated to state and NCCC offices who are accountable by policy for conducting a periodic reconciliation of IT assets, as well as communicating IT inventory changes to OIT.

Through periodic software updates that the Corporation pushed to user laptops and desktops through LANDesk, the Corporation is able to verify that the network components in their inventory exist.

[50] For text of this prior-year finding, please refer to page 35 of the published Office of Inspector General (OIG) Report 16-03, *Federal Information Security Modernization Act (FISMA) Evaluation of CNCS* for FY 2015.

FY 2015 – FISMA – NFR 4: Inaccurate Inventory of Physical IT Asset [50]

Although the Corporation made steps towards strengthening the management of its IT asset inventory, weaknesses remain in the implementation of the inventory processes. Specifically, the Corporation did not produce evidence that it performed a biannual physical IT inventory audits at HQ and field offices to ensure the IT inventory list and assignments of physical IT assets were accurate.

Discrepancies between the Corporation's expected inventory and the AmeriCorps Pacific NCCC and Seattle, WA state offices' current inventory served as additional proof that improvements are needed to the Corporation's inventory reconciliation process. During these visits, Kearney identified several discrepancies between the Corporation's and sites' IT asset inventory records. Specifically, some items with the status of "In Use" were found in boxes in storage closets. Two inventory assets did not have asset tags, and another was improperly labeled using another asset's ID tag.

As a result of not implementing the Corporation's inventory process to maintain a complete, accurate, and up-to-date IT inventory, the Corporation cannot diligently protect against waste, fraud, and abuse of IT assets. If items no longer in use are retained as active in the IT asset inventory, the Corporation could pay unnecessary software licensing fees for laptops and desktops that are not used.

FY 2015 Recommendations	FY 2016 Status
FY 2015 – FISMA – NFR 4 – Rec #1: Continue with the current plan to implement a single, centralized database to manage agency-wide physical inventory	Closed
FY 2015 – FISMA – NFR 4 – Rec #2: 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	Closed
FY 2015 – FISMA – NFR 4 – Rec #3: Perform biannual physical IT inventory audits at HQ and field offices to ensure the IT inventory list and assignments of physical IT assets are accurate	In Progress
FY 2015 – FISMA – NFR 4 – Rec #4: Perform periodic validation of the IT asset inventory in comparison with active network devices to identify potentially missing laptops and desktops	Closed

APPENDIX C: MANAGEMENT RESPONSE TO DRAFT FISMA REPORT

Corporation for National and Community Service

NationalService.gov

December 20, 2016

TO: Kenneth Bach, Deputy Inspector General

FROM: Thomas R. Hanley, Jr., Chief Information Officer

SUBJECT: Request for Comments on the Office of Inspector General's (OIG's) Draft Report: Fiscal Year 2016 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service

Dear Mr. Bach:

The Corporation for National and Community Service (CNCS) appreciates the opportunity to review the draft report of Kearney and Company's Fiscal Year 2016 Federal Information Security Management Act (FISMA) evaluation. CNCS concurs with all of the conditions and recommendations in the draft and offers the following comments.

CNCS is committed to maintaining a strong and effective Cybersecurity Program and we appreciate Kearney's acknowledgement of our significant progress addressing the information security and privacy weaknesses identified in last year's FISMA 2015 evaluation. As we improve the Cybersecurity Program, we will continue to address any outstanding issues.

As recommended, CNCS has already started working on the two new weaknesses that were discovered in the evaluation. CNCS is working to better define configuration baselines for devices and is enhancing the configuration management procedures to adequately track deviations from those baselines. In addition, CNCS has already addressed many of the weaknesses associated with monitoring and remediation of server backup failures. An automated notification has been configured to send emails to System Administrators when backup issues occur. Failures are promptly investigated and corrected and backup jobs are rerun to ensure data integrity. CNCS is aware that more work is needed and is committed to correcting and improving issues identified in the evaluation.

CNCS's Office of Information Technology (OIT) has developed a strategic plan that is used as the basis for all IT-related decisions. This has allowed OIT to plan for future growth and properly track that growth throughout the project lifecycle. In addition, OIT Cybersecurity has a firm understanding of the security posture of all CNCS systems by actively managing the plan of actions and milestones (POAMs). As part of OIT's commitment to cybersecurity, there are several projects planned for fiscal year 2017 that focus on achieving OIT's first strategic goal: Fortify Cybersecurity. CNCS is confident that the progress made in FY 2016 will continue into the upcoming year.

If you have any questions regarding these comments on the OIG's draft FISMA evaluation report, please contact Thomas Hanley, CNCS Chief Information Officer, 202-606-6618 or Andrea Simpson CNCS Chief Information Security Officer, 202-606-6792.

Thomas R. Hanley Jr.

Thomas R. Hanley, Jr.
Chief Information Officer
CNCS

Attachment
Comments on the Office of Inspector General's (OIG) Draft Report: Fiscal Year 2016 Federal Information Security Modernization Act (FISMA) Evaluation

Cc: Jeffrey Page, Chief Operating Officer
Andrea Simpson, Chief Information Security Officer
Guy Hadsall, OIG Chief Technology Officer

APPENDIX D: 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 two site visits.

Kearney created a questionnaire and submitted it to the five NCCC campuses, a Federal Financial Management Center (FFMC), Volunteer Member Services Unit (VMSU) and two state offices. The questionnaire requested information that was incorporated into a risk assessment to determine which site visits would be evaluated in FY 2016. Information such as the number of information technology (IT) assets, handling of personally identifiable information (PII), and the physical location of the office was used for consideration. Based upon the risk assessment, the AmeriCorps Pacific Region NCCC campus and the Seattle, Washington state offices were selected for site visits.

We conducted field office assessments at the AmeriCorps Pacific NCCC Region campus[1] at Sacramento (McClellan), CA on July 28, 2016 and the Seattle, WA state office on July 29, 2016. As part of our assessment strategy, we performed walkthroughs of workspace and office suite areas to identify physical access controls, in addition to conducting walkthroughs to identify unsecured PII. Kearney's visits to these locations also included an evaluation of controls to ensure acceptable usage of Corporation network resources, physical security, potential rogue connections (e.g., wireless access points, personal laptops), PII management, and a search for inappropriate material on a sample of Corporation workstations.

At each location, Kearney toured the facilities and noted the physical locations for storage of PII (paper and portable electronic). We noted that all locations stored PII records in locked file cabinets within locked rooms. Kearney noted that both offices dispose of PII in accordance with the retention schedules approved by the Corporation's policies and National Archives and Records Administration (NARA), as well as in accordance with agency litigation holds, which may require the retention of specific records until the litigation is resolved.

Kearney also noted IT inventory discrepancies at both the Pacific Region NCCC campus and the Seattle, WA state office. Please see Appendix B for further details. We noted the process to reconcile inventory once a year may lead to an inaccurate inventory. This issue was previously identified in FY 2015 FISMA finding, *Inaccurate Inventory of Physical IT Assets*, and repeats again in FY 2016.

[1] The AmeriCorps NCCC Pacific Region maintains a student/member computer lab and network similar to other AmeriCorps NCCC facilities. The equipment, software, and network were found to be separate from the CNCS network.

Finally, Kearney identified that the AmeriCorps Pacific NCCC campus maintains its own local area network to support NCCC member needs and a closed circuit television and physical security system. The local area network supports a computer lab and security system that are not managed by the Corporation’s Office of Information Technology. Kearney communicated our concerns that security patches and other security software may not be kept current to the Corporation’s management as observations.