Office of Inspector General
Corporation for NATIONAL & COMMUNITY SERVICE

November 14, 2014

TO: Jeffrey Page
Chief Operating Officer

FROM: Stuart Axenfeld
Assistant Inspector General Audit

SUBJECT: Federal Information Security Management Act (FISMA)
Independent Evaluation for FY 2014 (OIG Report Number 15-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 15-03 "FY14 Federal Information Security Management Act (FISMA) Evaluation for the Corporation for National and Community Service." This evaluation was performed by Kearney & Company, P.C. in accordance with the Quality Standards for Inspection and Evaluation promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE).

Kearney & Company, P.C. has concluded that the Corporation's Information Security and Privacy Program was not compliant in a number of respects with FISMA legislation, OMB guidance, and applicable NIST security publications as of September 30, 2014. Their testing found the controls were ineffective in seven of the 12 areas. In four of the seven areas, the deficiencies were severe enough to constitute a significant deficiency; these areas were Continuous Monitoring Management, Risk Management, Plans of Action and Milestones (POA&M), and Privacy.

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

Attachment

cc:
Tom Hanley, Chief Information Officer (Acting)

Office of Inspector General
Corporation for National and Community Service

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

INDEPENDENT EVALUATION FOR FY 2014

OIG REPORT 15-03

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

(202) 606-9390

This report was issued to Corporation management on November 14, 2014. Under the laws and regulations governing audit follow-up, the Corporation is to make final management decisions on the report's findings and recommendations no later than May 14, 2015, and complete its corrective actions by November 14, 2015. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

OIG Highlights

Objective

The Federal Information Security Management Act of 2002 (FISMA) requires each Federal agency to undergo an annual independent evaluation of its information security program and practices. The OIG contracted with Kearney to conduct the fiscal year (FY) 2014 FISMA evaluation of the Corporation. The objectives were to evaluate a representative subset of the Corporation's information systems for compliance with FISMA, OMB and NIST guidance and to evaluate the operating effectiveness of the information security and privacy controls over those systems.

Recommendations

Resolving serious security and privacy weaknesses throughout the Corporation's information security program will require a disciplined and sustained effort, as well as commitment of substantial resources. The OIG recommends that the Corporation take four key steps: (1) Establish an information technology project to prioritize and remedy the weaknesses, led by a Project Manager; (2) Develop a Project Plan, with specific milestones and assignments of responsibility; (3) Identify and marshal the resources, skills and expertise necessary to implement the plan; and (4) Establish performance metrics for information security. Oversight and support from agency leadership is crucial to that effort.

November 2014

Office of Inspector General
Corporation for NATIONAL & COMMUNITY SERVICE

Information Security and Privacy Program at the Corporation for National and Community Service Requires Great Improvement

What the OIG Found

The information security and privacy program at the Corporation for National and Community Service (Corporation) does not meet minimum standards and needs substantial improvement across the board. Kearney & Company, P.C. (Kearney), under the Office of the Inspector General's (OIG) supervision, uncovered weaknesses in 11 of the 12 areas tested. The controls were found to be ineffective in seven of these areas, and in four of them—Continuous Monitoring, Risk Management, Plans of Action & Milestones and Privacy—the defects were severe enough to constitute a significant deficiency, requiring immediate correction and attention by agency leadership. Five of these findings were recurring from last year. A review of the Department of Homeland Security's 115 security metric questions, divided into 11 subjects, identified 49 instances of non-compliance with applicable laws, regulations and authoritative guidance governing information security. Kearney also found significant weaknesses in Corporation's privacy controls for protection of Personally Identifiable Information (PII). Notably, Kearney concluded that the Corporation did not exercise meaningful oversight of the security measures by the contractors to whom it outsources its critical IT functions.

FY 2014 FISMA Evaluation Results

2014 DHS IG FISMA Reporting Area and Privacy	# of DHS Exceptions / Total DHS IG Questions	Severity of Noted Exceptions
1. Continuous Monitoring Management	8 of 8	Significant Deficiency
2. Configuration Management	7 of 13	Control Deficiency
3. Identity and Access Management	1 of 12	Control Deficiency
4. Incident Response and Reporting	2 of 9	Control Deficiency
5. Risk Management	10 of 17	Significant Deficiency
6. Security Training	2 of 7	Control Deficiency
7. POA&Ms	6 of 9	Significant Deficiency
8. Remote Access Management	1 of 13	Control Deficiency
9. Contingency Planning	8 of 13	Control Deficiency
10. Contractor Systems	4 of 8	Control Deficiency
11. Security Capital Planning	0 of 6	N/A
12. Privacy	N/A	Significant Deficiency

The Corporation took steps to correct certain of the deficiencies and has promised a plan for addressing others. However, throughout the evaluation field work, the Corporation maintained that its security program met all applicable standards, disagreed with Kearney's assessment of the severity of noted weaknesses, and questioned the value of adopting and documenting comprehensive policies and procedures for information security.

Fiscal Year 2014 Federal Information Security Management Act Evaluation for the Corporation for National and Community Service

November 14, 2014

Point of Contact:
Tyler Harding, Principal
1701 Duke Street, Suite 500
Alexandria, VA 22314
703-931-5600, 703-931-3655 (fax)
Tyler.Harding@kearneyco.com
Kearney & Company's TIN is 54-1603527, DUNS is 18-657-6310, Cage Code is 1SJ14

TABLE OF CONTENTS

Page #

KEARNEY& COMPANY

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

1. COVER LETTER

November 14, 2014

Wendy Spencer
Chief Executive Officer
Corporation for National and Community Service
1201 New York Avenue, NW, Suite 830
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 (Corporation) Information Security Program and practices. The Federal Information Security Management Act of 2002 (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 requires the Corporation to undergo an annual independent evaluation of its Information Security Program and practices, as well as an assessment of its compliance with the requirements of FISMA. The Corporation's Office of Inspector General (OIG) contracted with Kearney to perform an independent fiscal year (FY) 2014 FISMA evaluation of the Corporation's information technology (IT) policies, procedures, and practices. We are pleased to provide this FY 2014 FISMA Independent Evaluation Report, which details the results of our review of the Corporation's Information Security Program.

The objectives of the evaluation were to:

- Determine the efficiency and effectiveness of the Corporation's IT policies, procedures, and practices;
- Review a representative subset of the Corporation's information systems;
- Assess the Corporation's compliance with FISMA and related information security policies, procedures, standards, and guidelines;
- Evaluate personally identifiable information (PII) protection and privacy controls
- Evaluate physical controls at field office sites; and
- Prepare the Corporation's responses to the Department of Homeland Security's (DHS) *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics v1.0*, dated December 2, 2013.

Kearney's methodology for the FY 2014 FISMA evaluation included testing a sample of security controls over the Corporation's Local Area Network (LAN)/Wide Area Network (WAN) General Support System (GSS) and Electronic-System for Programs, Agreements, and National Service Participants (eSPAN) for compliance with the National Institute of Standards and Technology's (NIST) Special Publications (SP) and Office of Management and Budget (OMB) guidance; with emphasis on NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation*, promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE), and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

Based on our work performed, we concluded that the Corporation's Information Security and Privacy Program was not compliant in a number of respects with FISMA legislation, OMB guidance, and applicable NIST security publications as of September 30, 2014. A FISMA evaluation is required to address 11 specific aspects of information security, subdivided into 115 individual security metrics. In addition to the 11 FISMA metric areas, privacy controls were evaluated as a separate area for a total of 12 areas reviewed. **Our testing found the controls were ineffective in seven of the 12 areas. In four of the seven areas, the deficiencies were severe enough to constitute a significant deficiency; these areas were Continuous Monitoring Management, Risk Management, Plans of Action and Milestones (POA&M), and Privacy.** OMB M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, defines a significant deficiency as:

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

Of the 115 metrics, our testing identified 49 instances of noncompliance with OMB guidance and NIST SPs, itemized in Appendix E, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*. These instances of noncompliance are grouped into 16 findings. This report includes 67 recommendations, some of which overlap, to strengthen the Corporation's Information Security Program. Kearney considers seven of the 16 findings to be high risk and has classified them as significant deficiencies following OMB's annual FISMA reporting instructions as these findings require the attention of agency leadership and immediate or near-immediate corrective actions.

In response to our reported findings, the Corporation began taking steps to correct noted control deficiencies. Kearney recognizes that the Corporation is operating in an environment of constrained personnel resources and limited funding, as well as planning to modernize its IT

KEARNEY& COMPANY

infrastructure and eSPAN application. Resolution of all noted security weaknesses within a single year may be impractical, considering such limitations and other operational priorities.

To address such realities, Kearney offers the following four broad suggestions to help the Corporation chart an efficient course to achieve reasonable assurance of adequate security.

1. Establish an IT project to prioritize and remediate the noted IT security weaknesses and assign a Project Manager;
2. Develop a project plan, inclusive of tasks, milestone dates, and assignments of responsibility;
3. Identify the resource skills, associated experience levels, and financial resources necessary for successful implementation of the project plan; and
4. Establish performance metrics for information security, with periodic (not less than quarterly) briefings for executive leadership on the metric results and the status of the IT project's efforts to remediate known weaknesses.

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

For the Corporation's reference, we have included detailed information in a series of appendices. Appendix A, *Notices of Findings and Recommendations,* provides the full text of each FISMA finding. Appendix B, *Status of Prior Year Findings*, reviews the current status of findings and recommendations from prior years. Appendix C, *Management's Response*, provides the Corporation's response to the draft FISMA report. Appendix D, *Kearney and OIG Comments on Planned Actions,* indicates whether the Corporation's planned actions are responsive to noted weaknesses and recommendations. Appendix E, *Responses to DHS FY 2014 Inspector General FISMA Reporting Metrics,* contains responses to each of DHS's 115 security metrics.

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

Sincerely,

Kearney & Company, P.C.
November 14, 2014

2. BACKGROUND

2.1 Corporation Overview

In 1993, the Corporation was established to connect Americans of all ages and backgrounds with opportunities to give back to their communities and the nation. Its mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. The Corporation's Board of Directors and Chief Executive Officer (CEO) are appointed by the President and confirmed by the Senate. The CEO oversees the agency, which employs approximately 650 employees operating throughout the United States and its territories. The Board of Directors sets broad policies and direction for the Corporation and oversees actions taken by the CEO with respect to standards, policies, procedures, programs, and initiatives, as are necessary to carry out the mission of the Corporation.

2.2 Information Technology Overview

The Corporation relies on IT systems to accomplish its mission of cost-effectively providing and managing volunteer services nationally; it strives to deliver world-class customer service at the lowest cost without sacrificing service levels, quality, or any disruption or degradation of services. The Corporation has an inventory of 10 information systems. The Federal Information Processing Standard (FIPS) Publication (PUB) 199[1] security categorization levels of these systems are moderate (eight of 10 systems) and low (two of 10 systems). Of the 10 information systems, nine are hosted and operated by third-party service providers. The Corporation's network consists of multiple sites: Headquarters (HQ), one Field Financial Management Center, five National Civilian Community Corps (NCCC) campuses, one Volunteers in Service to America (VISTA) Member Support Unit (VMSU) campus, and many state offices in cities throughout the United States. These sites are interconnected with high-speed network connections.

Sustaining high levels of service at low costs is challenging for the Corporation. The Corporation determined that outsourcing its IT infrastructure, while at the same time implementing changes in IT governance, would provide the highest-quality systems at the lowest cost. Contractors were sought to manage the Corporation's three primary information systems:

1. 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. This includes:

[1] FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* provides standards for Federal agencies to classify their information systems based the data types an information system processes and the potential impact on an organization should certain events occur that jeopardize the information and the information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, and maintain day-to-day functions.

- Data center services, such as server services, middle-ware 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; and engineering; facility and environmental infrastructure; operations, administration, and maintenance of infrastructure; and IT Infrastructure Library (ITIL)-based service management processes

2. eSPAN – eSPAN is a custom web application based on an Oracle database for the National Service Trust (TRUST) and Participant Systems. The system tracks AmeriCorps members and TRUST educational awards, including awards made to all individuals in the 20-year history of the Corporation (approximately 1.2 million individuals); and
3. Momentum – Momentum is a multi-tier, distributed, commercial off-the-shelf (COTS) enterprise financial management software system supporting data exchange with other Federal systems, providing financial planning capabilities and a means to record the agency's financial transactions. Momentum is the official system of record for financial management at the Corporation. Momentum 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.

The Corporation implemented its outsourcing strategy as a way to achieve higher quality at lower costs; however, the budget environment in the Federal community has become increasingly strained. According to the Corporation's Chief Information Officer (CIO), its Information Assurance Program (IAP) remained fully funded while other areas of the Corporation sustained budget decreases resulting from sequestration. However, Kearney observed that: (1) the Corporation removed previous contract requirements for independent security assessments to achieve mandatory cost reductions from its MDCS IT vendor; and (2) the Corporation left vacant a full-time equivalent position for an Information Security Specialist position for approximately eight months and chose not to backfill the position with temporary contractor support. These circumstances highlight the difficult operational choices that the Corporation must make in an environment with limited funding.

The Corporation's outsourcing strategy directly influences how it implements required information security controls. Outsourcing is not inherently detrimental to the security posture of the organization, but it does introduce different considerations and new risks regarding the protection of information and information systems. While the Corporation elected to outsource a significant share of IT functions, by law it retains responsibility for complying with the requirements of FISMA and security control implementation. As the Corporation looks to the future by embracing cloud computing, re-competing the MDCS contract, and completing the implementation of Microsoft Office 365, the Corporation should consider the recommendations presented in this report.

2.3 FISMA

FISMA was enacted into United States Federal law under Title III of the E-Government Act of 2002 (E-Gov) Public Law (P.L.) 107-347 (December 17, 2002), 44 United States Code (U.S.C.) §§ 3541-49. FISMA outlines the information security management requirements for agencies, including the requirement for an annual evaluation by each agency's Inspector General (IG) or an independent external auditor. The annual independent evaluations are intended to inform agency management, OMB, Congress, and the American public on the effectiveness of the agency's Information Security Program and compliance with the FISMA legislation. The results of the evaluation must be reported to OMB and Congress, utilizing an automated reporting tool, CyberScope, no later than November 15 of each year.

Key requirements of FISMA legislation include:

- The development, documentation, and implementation of an agency-wide Information Security Program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source;
- An annual independent evaluation of the agency's Information Security Program and practices, as well as an assessment of its compliance with the FISMA requirements; and
- Tests of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems.

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

- Information security policies, procedures, standards, and guidelines;
- Delegation of authority to the CIO to ensure the design and implementation of information security policies are consistent with OMB and the NIST guidance;
- Security awareness training programs;
- Periodic testing and evaluation of the effectiveness of security policies, procedures, and practices, to be performed no less than annually;
- Periodic risk assessments;
- Processes to manage remedial actions for addressing deficiencies;
- Procedures for detecting, reporting, and responding to security incidents;
- Plans to ensure continuity of operations; and
- Annual reporting on the adequacy and effectiveness of the Information Security Program to OMB and Congress.

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

officials with prioritizing corrective action and resource allocation using a formal POA&M process.

2.3.1 NIST Security Standards and Guidelines

FISMA requires NIST to establish minimum standards and guidelines for Federal information systems, and further requires Federal agencies to comply with FIPS issued by NIST. The FIPS requirements are mandatory and cannot be waived. NIST also develops and issues SPs 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The purpose of NIST SP 800-53 is to provide guidelines for selecting and specifying security and privacy controls for information systems supporting an agency in meeting the requirements of FIPS PUB 200.

2.3.2 DHS FISMA Responsibilities

Under the authority of OMB, DHS facilitates the annual reporting of the CIO Reporting Metrics, Senior Agency Official for Privacy Reporting Metrics, and OIG Reporting Metrics to Congress, utilizing an online tool called CyberScope. For the OIG to prepare their annual responses using CyberScope, DHS provides instructions in the *FY 2014 IG FISMA Reporting Metrics* and requires each agency OIG to respond to 115 FISMA metric questions in 11 metric areas. Appendix E, *Responses to DHS's FY 2014 IG FISMA Reporting Metrics*, contains the OIG's responses for the Corporation. ***Exhibit 1: Summary of FY 2014 DHS IG FISMA Responses*** in **Section 3. RESULTS**, lists the 11 FISMA metric areas and provides Kearney's test results.

2.4 Scope

Kearney's independent evaluation of the Corporation's Information Security Program was conducted from May through September 2014. Our evaluation methodology met the *Quality Standards for Inspection and Evaluation* promulgated by CIGIE and included inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls. The FISMA evaluation included an assessment of the following:

- The Corporation's Information Security and Privacy Program activities;
- Management oversight of contractor-managed systems, including the Corporation's network and My AmeriCorps Portal;
- FY 2014 OMB/DHS reporting metrics; and
- Site visits to two Corporation State Offices (Texas and Iowa), the NCCC North Central Region, and the VMSU.

3. RESULTS

To assess the operating effectiveness of the Corporation's agency-wide information security and privacy program and practices as required by FISMA, Kearney performed detailed testing of the Corporation's GSS and one application for compliance with selected NIST SP 800-53 controls. **From our sampling, we found that the Corporation was non-compliant with FISMA legislation, OMB guidance, and NIST SPs in 49 of 115 security metric areas, as shown in *Exhibit 1* below.**

This section provides the conclusions of our research, analysis, and assessment of the Corporation's information security and privacy program, policies, and practices. Authoritative policies, standards, and guidance are cited where applicable. As shown in ***Exhibit 1*** below, Kearney concluded that management attention is needed to address deficiencies (some significant deficiencies and urgent) in 10 of the 11 DHS security areas and privacy controls.

Exhibit 1: Summary of FY 2014 DHS IG FISMA Responses

2014 DHS IG FISMA Reporting Area and Privacy	Controls Effective Overall (Yes/No)	# of DHS Exceptions / Total DHS IG Questions	Severity of Noted Exceptions
1. Continuous Monitoring Management	No	8 of 8	Significant Deficiency
2. Configuration Management	No	7 of 13	Control Deficiency
3. Identity and Access Management	Yes	1 of 12	Control Deficiency
4. Incident Response and Reporting	Yes	2 of 9	Control Deficiency
5. Risk Management	No	10 of 17	Significant Deficiency
6. Security Training	Yes	2 of 7	Control Deficiency
7. POA&Ms	No	6 of 9	Significant Deficiency
8. Remote Access Management	Yes	1 of 13	Control Deficiency
9. Contingency Planning	No	8 of 13	Control Deficiency
10. Contractor Systems	No	4 of 8	Control Deficiency
11. Security Capital Planning	Yes	0 of 6	N/A
12. Privacy†	No	N/A	Significant Deficiency

† – Consistent with the addition of privacy controls to NIST SP 800-53, Revision 4, the OIG contracted with Kearney to evaluate the Corporation's implementation of specific privacy controls as part of the FY 2014 FISMA evaluation.

In response to draft Notices of Findings and Recommendations (NFR), the Corporation stated in its opinion that it has adequately adapted the standards and guidance to meet the needs of a small

agency in a cost-effective manner. While FISMA contemplates "information security protections commensurate with the risk and magnitude of the harm," mandatory requirements may not be waived.[2] Given the significant quantities of PII that the Corporation collects in fulfilling its mission, its information systems must be well-protected, using the NIST SP 800-53, Revision 4 security controls catalog for moderate-impact systems and other applicable guidance.

As ***Exhibit 1*** illustrates, 11 of the 12 areas evaluated warrant additional management attention to address identified deficiencies. Five of the findings are repeats from the FY 2013 FISMA evaluation. Our findings are summarized below:

Continuous Monitoring Management

1. *Lack of a formally documented and fully implemented Information Security Continuous Monitoring (ISCM) strategy (Repeat finding from FY 2013 FISMA evaluation)*
   Severity: Significant Deficiency
   The Corporation has not adopted, formally documented, and implemented an organization-wide ISCM strategy and program. As part of monitoring its outsourced information systems, the Corporation has not developed meaningful and reportable performance metrics to evaluate the IT contractors' performance and incorporated such performance metrics into its IT contracts.

2. *Multiple weaknesses with vulnerability scanning and remediation*
   Severity: Significant Deficiency
   Kearney identified five deficiencies related to vulnerability scanning and the remediation process at the Corporation. Specifically, the Corporation did not:
   a. Scan desktops and laptops on a monthly basis for missing security patches and/or configuration errors;
   b. Review monthly scan results of servers for 10 months. As a result, this allowed 39 high-risk vulnerabilities to continue for this period;
   c. 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;
   d. Periodically perform a scan for configuration errors and deviations from the United States Government Configuration Baseline (USGCB) for desktops; and
   e. Include performance metrics for the timely remediation of identified vulnerabilities in the MDCS or other IT contracts.

[2] 44 U.S.C. § 3544(a).

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

4. *Use of an obsolete and unsupported network monitoring tool*
   Severity: Significant Deficiency
   The Corporation's primary tool for network monitoring and audit log analysis is obsolete and unsupported by the vendor. Additionally:
   a. The Corporation did not have a standard operating procedure requiring the periodic review and maintenance of the primary network monitoring and audit log tool, which had not been reviewed and tuned for the audit alerts in more than two years;
   b. The monitoring tool did not retain audit events for a long enough period to allow useful aggregation to identify trends and perform targeted analysis; and
   c. The Corporation 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.

<u>Configuration Management</u>

5. *Lack of controls to prevent use of unauthorized devices*
   Severity: Control Deficiency
   The Corporation did not implement IT security policies and supporting technical controls to prevent the use of non-Corporation issued portable data storage devices such as Universal Serial Bus (USB) thumb drives, USB hard drives, smart phones, and tablets. Further, Kearney observed Corporation employees utilizing personal devices for work purposes even though the Corporation did not have a bring-your-own-device (BYOD) policy that permitted such behavior. The Rules of Behavior discuss removable storage media in regard to encrypting PII or sensitive information did not directly address BYOD devices. Also, the Corporation did not require employees and contractors to use federally approved cryptographic algorithms to store PII.

6. *Risks to the confidentiality and availability of Voice Communications*
   Severity: Control Deficiency
   The Corporation does not separate its data network traffic from its voice network traffic. Specifically, Corporation desktops were able to ping (query) Cisco Voice over Internet Protocol (VoIP) phones at remote offices. In addition, users were able to access the Cisco VoIP phones using their desktops' web browser over hypertext transfer protocol (HTTP). The connectivity between the data and voice virtual local area networks (VLAN)[3] could be exploited by malicious individuals to compromise VoIP components, which generally were not designed with security in mind, and could allow an attacker to intercept and record phone calls.

Identity and Access Management

7. *Lack of segregation of duties*
   Severity: Control Deficiency
   The Corporation did not document requirements for segregation of duties (SoD) for the eSPAN application. This issue has been recurring for the past four years. Despite repeated assurances that the Corporation is in the process of establishing required segregation of duties across all business processes, and aligning this with its IT systems, the Corporation has not demonstrated meaningful progress to resolve the weakness.

Incident Response and Reporting

8. *Inadequate incident response reporting*
   Severity: Control Deficiency
   The Corporation has not properly classified all computer security incidents, nor has it reported all computer security incidents to the United States-Computer Emergency Readiness Team (US-CERT). Specifically, three Category 1 events and three Category 4 events[4] were not reported because they were not correctly classified as reportable events.

[3] According to Cisco, a VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire when, in fact, they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible. VLANs are usually associated with IP sub-networks. For example, all the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. VLAN port membership is assigned manually on a port-by-port basis.

[4] Category 1 events represent unauthorized access and must be reported within one hour of discovery. Unauthorized access occurs when an individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource. Category 4 events represent improper usage and must be reported weekly. Improper usage occurs when a person violates acceptable computing use policies.

Risk Management

9. *Inadequate enterprise-wide risk management policies and practices (Repeat finding from FY 2013 FISMA evaluation)*
   Severity: Control Deficiency
   The Corporation's documented risk management policies and security controls described the risk management process at the information system (Tier 3) level but do not address risks at Tier 1 (Organization) and Tier 2 (Mission/Business). The risk management practices largely do not involve the individuals who are responsible for 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. The Corporation disagreed with the observation and stated that risk management occurs at Tier 1 and Tier 2 as part of their change management process, but agreed that risk management practices were not formally documented.

10. *Weaknesses with the Corporation's security planning and assessment process (Repeat finding from FY 2013 FISMA evaluation)*
    Severity: Significant Deficiency
    The Corporation did not develop corporate standards for its multiple IT contractors to follow regarding ongoing security assessments and continuous monitoring activities. Kearney's testing of IT security controls across a multitude of the Corporation's information systems identified multiple inconsistencies and inaccuracies in the SSPs, SARs, and POA&Ms, highlighting the inconsistent nature, depth, and quality of security assessments and continuous monitoring activities performed by the Corporation's IT vendors.

    While the Corporation has provided some high-level guidance, it did not provide detailed instructions to ensure consistency and compliance with NIST guidance when conducting security assessments. Specifically, the Corporation:
    a. Has not developed standard test cases;
    b. Has not developed a sampling plan for testing;
    c. Has not documented its approach for testing common controls or how the Corporation assesses required security controls that are not within the scope of the IT service provider's information systems;
    d. Has not specified when security assessor independence and impartiality is required and when it may be waived;
    e. Did not require its security control assessors to compare the implementation details from the SSP to actual practice and note any discrepancies; and
    f. Did not use established templates for Acceptance of Risk for all identified and accepted risks.

Security Training

11. *Lack of formal, role-based training (Repeat finding from FY2013 FISMA evaluation)*
    Severity: Control Deficiency
    The Corporation has not implemented a formal, documented, role-based Information Security Training program that includes regular training updates.

POA&Ms

12. *Improvements needed to POA&M Reporting (Repeat finding from FY2013 FISMA evaluation)*
    Severity: Significant Deficiency
    The Corporation did not have an adequate POA&M management process in place to ensure that all known security weaknesses are recorded, remediation resources are identified, and progress toward timely resolution is adequately monitored. The Corporation's POA&Ms did not identify resources required to resolve open tasks, such as estimating the level of effort in man-hours or other costs to procure contractor support or tools.

Remote Access Management

13. *Inadequate controls over remote access*
    Severity: Control Deficiency
    The Corporation-issued laptops were configured to automatically connect to the Corporation's network through Cisco's "AnyConnect VPN" client. However, the automatic connection of the laptop to the Virtual Private Network (VPN) server does not meet the two-factor authentication requirements for Federal agencies where "one of the factors is provided by a device separate from the computer gaining access."[5] In addition, the Corporation incorrectly configured its VPN to permit the use of non-compliant, FIPS[6] encryption protocols,[7] leaving VPN sessions vulnerable to exploitation, such as "man-in-the-middle attacks." Kearney also noted that the Corporation's VPN client did not include the latest Cisco security patches as of August 25, 2014 to several Secure Socket Layer (SSL)/Transport Layer Security (TLS) vulnerabilities.

Contingency Planning

14. *Inadequate Disaster Recovery Plan (DRP) documentation and planning*
    Severity: Control Deficiency
    The Corporation's Disaster Recovery documentation does not plan for all of the Corporation's essential functions and missions. The Business Impact Analysis (BIA) specifically states that it is not meant to address all essential business functions, and refers to the Continuity of Operations Plan (COOP) and the Corporation DRP for

[5] OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006.
[6] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.*
[7] RC4, SSL 3.0, and SSL 3.1/TLS 1.0. RC4, SSL 3.0, and TLS 1.0 are widely used commercially, but have several technical flaws that can increase the risk of exploitation.

coverage. However, the COOP and DRP also did not identify all essential business functions. Further, the Corporation's DRP is written specifically for the MDCS; it is not representative of the Corporation as a whole and did not acknowledge other key IT contractors and systems. Based on review of available BIAs, DRPs, and COOP documentation, the Corporation has a gap in the its COOP and consideration of essential business functions.

15. *Lack of Adequate testing of COOP*
Severity: Control Deficiency
The Corporation has not conducted adequate planning or testing of its COOP. The following aspects of the Corporation's COOP and DRPs make it inadequate:
   a. The COOP does not include sufficient information to address all mission-essential functions and subordinate plans and details that would be necessary should the plan ever need to be activated;
   b. The Corporation has made assumptions that do not appear reasonable should it be necessary to activate the COOP, such as all vital records are available electronically and all employees, supporting essential business functions, have laptops; and
   c. Evidence of annual COOP testing, including after-action reports, as required for mission essential functions and the agency's financial system did not exist.

Contractor Systems

The election to outsource significant IT functions does not relieve the Corporation of its responsibility to comply with the requirements of FISMA and security control implementation. To provide greater detail, Kearney has reported issues arising from contractor systems under the specific FISMA metric area rather than under the Contractor Systems metric, because nearly all of the relevant systems and functions have been outsourced. In the majority of these cases, the Corporation did not exercise sufficient oversight of critical contractor functions.

Security Capital Planning

Controls in the area of security capital planning were considered effective, and no reportable deficiencies were identified.

Privacy

16. *Inadequate controls over Privacy*
Severity: Significant Deficiency
The Corporation demonstrated multiple weaknesses in the implementation of privacy controls including:
   a. The Corporation has not explicitly documented its privacy controls, as required by Appendix J of NIST SP 800-53;
   b. The Corporation has not fully documented its PII inventory;
   c. The Corporation employees did not comply with requirements to destroy outdated records containing PII in accordance with the Record Retention Schedule promulgated by the National Archives and Records Administration (NARA); and

d. The Privacy Impact Assessments (PIA) for two key information systems, Momentum and eSPAN, have not been updated since 2009 and were not publicly posted on the Corporation's website.

Addressing these deficient security practices will strengthen the Corporation's Information Security Program and contribute to ongoing efforts to achieve reasonable assurance of adequate security over information resources. Below, Kearney offers several broad recommendations to that end. The NFRs reported in Appendix A contain more specific recommendations. As of September 2014, the Corporation had begun taking steps toward strengthening controls in some of these areas, as noted in each NFR. Overall, to improve its Information Security and Privacy Program, the Corporation should take the following key steps:

1. Establish an IT project to remediate the noted IT security weaknesses and assign a Project Manager;
2. Develop a project plan, inclusive of tasks, milestone dates, and assignments of responsibility;
3. Identify the resources, skills, experience levels, and financial resources necessary for successful implementation of the project plan;
4. Establish performance metrics for information security, with periodic (not less than quarterly) briefings for executive leadership on the metric results and the status of the IT project's efforts to remediate known security and privacy weaknesses;
5. Improve the risk management processes and information security policies to ensure they address all levels of the organization at the system level (Tier 3), business process level (Tier 2) and organization-wide (Tier 1);
6. Improve documentation in the following areas:
   a. Continuous monitoring plans, testing, and results,
   b. Risk management and acceptance,
   c. POA&Ms,
   d. Contingency planning, and
   e. Privacy
7. Improve policies and procedures, including those that will be used by all Corporation employees, through clarification, addition of details, and agency-wide standardization of processes;
8. Strengthen the oversight of contractors by:
   a. Ensuring contracts include proper IT clauses and provisions for information security, as well as Whistleblower Protection clauses for employees of Government contractors,
   b. Identifying the security controls that the contractor is responsible for implementing and then incorporating them into contracts and any task orders, and
   c. Establishing performance metrics inclusive of IT security metrics
9. Improve ISCM by:
   a. Implementing performance metrics to monitor progress and hold responsible parties accountable,
   b. Assigning responsibilities for implementing common and privacy controls to the Corporation and contracts,

   c. Establishing SA&A standards and templates to be used both by the Corporation and its IT contractors, and
   d. Refreshing technology to move closer to real-time monitoring
10. Review the technical aspects of the IT Security Program to ensure software patches are timely deployed, installed desktop configurations comply with the USGCB, deviations or vulnerable software configurations are identified and remediated timely, and unnecessary software and hardware is removed;
11. Improve training for information system users with significant security responsibility;
12. Enhance the POA&M process to track all deficiencies, prioritize remediation actions, and monitor resource needs; and
13. Improve contingency planning to ensure that the plans are clearly understood, actionable, tested, improved upon, and included assumptions are valid.

APPENDIX A: NOTICES OF FINDINGS AND RECOMMENDATIONS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our" in this report) issued 16 Notices of Findings and Recommendations (NFR) to the Corporation for National and Community Service (Corporation) as a result of the fiscal year (FY) 2014 Federal Information Security Management Act of 2002 (FISMA) Independent Evaluation. The 16 NFRs are presented in full in this appendix.

1. Continuous Monitoring Management

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

(*See Appendix E, related Department of Homeland Security [DHS] Question # 1: Continuous Monitoring Management)*

Background: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organization* defines ISCM as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." The publication further notes that an effective ISCM begins with development of a strategy that addresses ISCM requirements and activities at each organizational tier (i.e., organization, mission/business processes, and information systems). Each tier monitors security metrics and assesses security control effectiveness with established monitoring and assessment frequencies, and status reports customized to support tier-specific decision-making. The process begins with leadership defining a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people.[8]

Condition: The Corporation has not formally documented and implemented an organization-wide ISCM strategy and program, as mandated by the Office of Management and Budget (OMB) guidance and as required by several NIST SPs including NIST SP 800-137, NIST SP 800-37, Revision 1, NIST SP 800-39, and NIST SP 800-53, Revision 4. The Corporation has made a conscious decision to outsource its General Support System (GSS),[9] its major applications,[10] and its external public-facing websites to different commercial providers. To some extent, the Corporation relies upon each service provider to establish a continuous monitoring process. The Corporation has not, however, developed a comprehensive organization-wide ISCM process to provide effective oversight for developing,

[8] As stated in NIST SP 800-137, the strategy should be: 1) grounded in a clear understanding of organizational risk tolerance and help officials set priorities and manage risk consistently throughout the organization; 2) include metrics that provide meaningful indications of security status at all organizational tiers; 3) ensure continued effectiveness of all security controls; 4) verify compliance with information security requirements derived from organization missions/business functions, Federal legislation, directives, regulations, policies, and standards/ guidelines; 5) be informed by all organizational information technology (IT) assets and help maintain visibility into the security of the assets; 6) ensure knowledge and control of changes to organizational systems and environments of operation; and 7) maintain awareness of threats and vulnerabilities.

[9] The GSS for the Corporation includes the Local Area Network (LAN)/Wide Area Network (WAN).

[10] The major applications are Momentum and Electronic System for Program, Agreements, and National Service Participants (eSPAN). eSPAN includes the eGrants application and My AmeriCorps Portal.

implementing, and operating these individual systems in support of the Corporation's core missions and business processes.

Kearney reviewed the Corporation's Information Assurance Program (IAP)[11] and noted that the document briefly addresses ISCM. However, the ISCM Program did not have processes in place to support ISCM across the entire organization; the Corporation's IAP described an ISCM Program operated at Tier 3 (Information Systems) and was focused on contractor-provided services and did not address Tier 1 (Organization) and Tier 2 (Mission/Business Processes). The Corporation implemented several tools[12] that provide continuous monitoring. While, the Corporation used the weekly Production Change Control Board (PCCB) meeting to discuss organization-wide issues that require changes, these meetings focus on technical changes to information systems and not the broader issues involved with continuous monitoring. Further, the Corporation has an Executive Review Board (ERB) involving individuals outside of the Office Information Technology (OIT); the ERB focused on IT acquisitions, not continuous monitoring.

Additionally, IAP did not identify performance metrics that were meaningful and reportable for all business processes supporting the Corporation's mission. Kearney noted this same issue in the FY 2013 FISMA report. Since the FY 2013 FISMA evaluation, the Corporation has continued to focus on information system-level ISCM and has not established a comprehensive, organization-wide ISCM Program for the Corporation's IT environment.

Criteria: In 2009, OMB and NIST recognized that the existing Government-wide approach of reassessing all GSS and major applications every three years, as required by OMB Circular A-130, Appendix III, did not address the dynamic nature of IT and the constantly changing threat landscape to the organization, business/mission, and supporting information systems. OMB and NIST therefore determined that agencies needed to develop near-real-time continuous monitoring practices. OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the FISMA and Agency Privacy Management,* provides specific guidance regarding continuous monitoring and risk management practices. OMB states in its Frequently Asked Questions:

> # 34: Is a security reauthorization still required every 3 years or when an information system has undergone significant change as stated in OMB Circular A-130? No. Rather than enforcing a static, three-year reauthorization process, agencies are expected to make ongoing authorization decisions for information systems by leveraging security-related information gathered through the implementation of ISCM programs. The implementation of ISCM and ongoing authorization thus fulfill the three-year security reauthorization requirement, so a separate re-authorization process is not necessary. In an effort to implement a more dynamic, risk-based security authorization process, agencies should follow the guidance in NIST Special Publication 800-37. Agencies will be required to report the security state of their information systems and results of their ongoing authorizations through CyberScope in accordance with the data feeds defined by DHS.

[11] *CNCS Information Assurance Program*, November 2012.

[12] The tools used by the Corporation include Solar Winds, Good, MARS 360, Symantec Validation, and Identity Protection Service.

OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the FISMA and Agency Privacy Management*, states:

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

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

- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. Security Control CA-7 "Continuous Monitoring" and related Security Controls RA-2, "Security Categorization," CA-2, "Security Assessment," and CA-6, "Security Authorization" discuss specific elements of ISCM;
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010. This SP discusses the NIST Risk Management Framework, which comprises six steps that provide a structured practice for incorporating information security and risk management activities into the system development lifecycle;
- NIST SP 800-39, *Managing Information Security Risk*, March 2011. This SP provides guidelines for developing an ISCM strategy and implementing an ISCM Program; and
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011. This SP describes the fundamentals of ongoing monitoring in support of risk management.

Cause: The Corporation has not adopted the current guidance from OMB and NIST regarding continuous monitoring and has only focused on Tier 3 ISCM, which addresses risk at the information systems level. As a result, there are gaps in the ISCM process at the Tier 1 (Organization) and Tier 2 (Mission/Business Processes) levels. The Corporation's Chief Information Officer (CIO) stated that, as a small agency, it does not need to document its Continuous Monitoring Program because doing so is not cost-effective or a good use of scarce resources. Further, the CIO stated that every security decision is made in the context of mission and the organization, thus additional documentation would not add value to the Corporation. Kearney respectfully disagrees that documenting an ISCM strategy is waste of the Corporation's resources as strategy documents communicate management priorities, policies, and attitudes toward risk. ISCM strategies also identify information security performance metrics, which inherently reflect management's goals.

Kearney noted in the FY 2013 FISMA report that the Corporation had not formally documented and implemented an organization-wide ISCM strategy, as mandated by OMB guidance and required by four NIST SPs. Since the FY 2013 FISMA evaluation, the Corporation has not made adequate progress implementing appropriate corrective actions.

Effect: Failure to implement a formally documented and implemented organization-wide ISCM strategy, including Tier 1 and Tier 2 levels, weakens the internal control environment and increases the risk that known information security weaknesses are not elevated to the business owners' attention and managed in conjunction with other business risks. Without performance metrics and regular reporting of security weaknesses to business owners, information security weakness could be left unaddressed and present an unacceptable business risk.

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

Recommendation: To improve the Corporation's ISCM strategy and to comply with OMB and NIST requirements, Kearney recommends that the Corporation:

1. Document and fully implement an organization-wide, comprehensive ISCM strategy that incorporates Tier 1 and Tier 2 levels;
2. Improve oversight over IT service providers; and
3. Formalize ISCM processes to include the following:
   a. Establishment of metrics to be monitored,
   b. Establishment of frequencies for monitoring/assessments,
   c. Approach for ongoing security control assessments and status monitoring to determine the effectiveness of deployed security controls,
   d. Correlation and analysis of security-related information generated by assessments and monitoring,
   e. Response actions to address the results of the analysis, and
   f. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.

Finding #2: Multiple Weaknesses with Vulnerability Scanning and Remediation
(*See DHS Question # 2: Configuration Management)*

Background: Vulnerability management is a key security control and practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation. Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have on a computer. One method for resolving security vulnerabilities involves deploying security patches. Patches are additional pieces of code developed to address security flaws within a program. Not all security vulnerabilities have related patches, and remediation activities may include device or network configuration changes to limit the exposure of a system to vulnerabilities. Major software vendors such as Microsoft, Adobe, and Oracle have implemented regularly scheduled security updates on a monthly and quarterly cycle with out-of-cycle releases occurring to address critical vulnerabilities. NIST recommends that Federal agencies and organizations prioritize software deployment and testing of security patches based on risk (i.e., critical, high, moderate, low) to an information system.

Federal agencies and organizations implement vulnerability scanning to confirm that their proactive efforts to deploy security patches were effective and to identify unknown vulnerabilities in their information systems. As these vulnerability scanning activities typically occur monthly following a deployment of security patches, Federal agencies and organizations use performance metrics to measure the effectiveness and timeliness of vulnerability remediation efforts. These performance metrics often identify the percentage of software patches successfully deployed to a target population (e.g., desktops) and measure the timeliness of software deployments such as identifying, testing, and deploying a security patch mitigating a high-risk vulnerability within an agreed-upon time frame (e.g., 10 days). OMB, DHS, and the NIST require Federal agencies to develop security metrics and incorporate these into their Continuous Monitoring Program.

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

- *Scan desktops and laptops on a monthly basis* – The Corporation's vulnerability scanning process, administered by its Managed Data Center Services (MDCS) provider, included only servers and routers. The Corporation's vulnerability scanning process did not include the Corporation's desktops or laptops;
- *Review monthly scan results of servers for 10 months, and as a result allowed 39 high-risk vulnerabilities to continue* – Although the Corporation and the MDCS contractor received monthly reports of identified vulnerabilities from its tool, McAfee Vulnerability Manager (MVM), neither the Corporation nor its MDCS contractor took actions to remediate the 39 high-risk weaknesses until at least 10 months after identification by Kearney during the FISMA audit;
- *Maintain the vulnerability scanner or configure the scanner to identify missing security patches belonging to applications* – The Corporation did not enable security checks that were designed to

detect missing application security patches[13] and out-of-date security software, as part of the monthly vulnerability scans for its Windows servers. OIT officials stated that there was concern over the intrusiveness of vulnerability detections; therefore, the security checks were set to a limited "non-intrusive" scan configuration. However, the Corporation acknowledged that it did not test to determine whether the more intrusive scans harmed server performance, if used during non-work hours;

- *Perform a scan for configuration errors and deviations from the United States Government Configuration Baseline (USGCB)* – The Corporation did not provide evidence of periodic scanning for USGCB compliance on its desktops and laptops; and
- *Establish the MDCS contract performance metrics for the timely remediation of identified vulnerabilities* – The Corporation had not established performance metrics for the MDCS contract related to the timely remediation of identified vulnerabilities.

Criteria: NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires Federal agencies and organizations to implement vulnerability scanning controls in RA-5 "Vulnerability Scanning." This control states, in part, that the organization scans for vulnerabilities in the information system and hosted application, analyzes vulnerability scan reports and results from security control assessments, and remediates legitimate vulnerabilities.

Closely related to vulnerability scanning is the remediation of detected vulnerabilities in NIST SP 800-53 security control SI-2 "Flaw Remediation." This control states, in part, that the organization identifies, reports, and corrects information system flaws; installs relevant software and firmware updates within a period defined by the organization[14] of the release of the updates; and incorporates flaw remediation into the organizational configuration management process, including performance metrics. As vulnerability scanning and remediation is an ongoing process, NIST SP 800-53, Revision 4, requires organizations to adopt performance measures in PM-6 "Performance Metrics." The control states that the organization should "… develop, monitor, and report on the results of information security measures of performance."

NIST SP 800-55, *Performance Measurement Guide for Information Security*, suggests multiple performance measures to measure the effectiveness of vulnerability identification and remediation process. Examples include percentage of high-, moderate-, and low-risk vulnerabilities remediated within an organizationally defined time period.

[13] The Corporation did enable security checks for some Windows Operation System (OS) patches, but did not confirm that all were enabled on a monthly basis.
[14] The Corporation has not defined this time period in the GSS system security plan (SSP).

Under the MDCS contract awarded by the Corporation:[15]

> The contractor is responsible for complying with all CNCS [Corporation] and Federal security requirements and shall ensure that its subcontractors (at all tiers) which perform work under this contract comply with all security requirements…
>
> 2. … The Contractor must configure its systems that contain Corporation data with the applicable United States Government Configuration Baselines (USGCB) and ensure that systems have and maintain the latest operating system patch and an updated anti-virus. The Contractor must use common security configurations available from the National Institute of Standards and Technology's (NIST) National Checklist Program Repository…
>
> 4. … The Contractor must comply with the following:
>
> - **Federal Information Security Management Act (FISMA) of 2002** (Title III of the E-Government Act of 2002 (E-Gov), Public Law 107-347)
> - **(OMB) Circular A-130** (Management of Federal Information Resources), Appendix III (Security of Federal Automated Information Resources)
> - **NIST Special (SP) and Federal Information Processing Standard (FIPS) Publications**
> - **CNCS [Corporation] Information Assurance Policies**.

Cause: The Corporation has not performed adequate contract oversight and enforced the provisions of the MDCS contract to ensure that vulnerability scanning tools are current, updated as necessary, and capable of identifying software vulnerabilities and configuration weaknesses in the Corporation's GSS LAN/WAN. The Corporation stated that preventive controls[16] existed to adequately remediate any identified weaknesses.

Specifically, in the order discussed above, Kearney noted five observations.

Observation 1 – After the departure of a Corporation Information Assurance employee in January 2014, the position remained unfilled as of September 2014. As a result, the Corporation stopped conducting vulnerability scans of the Corporation's laptops and desktops. The former Information Assurance professional performed vulnerability scans of servers and desktops using two different tools, MVM and Tenable's Nessus scanner. Upon his departure, the MDCS contractor partially assumed responsibilities for performing vulnerability scans using MVM, but not Nessus. The MDCS contractor did not review and update the list of vulnerability checks in the MVM scanner to ensure that all currently identified

[15]The contract was awarded to provide MDCS for the Corporation Document Number CNS09A0021-0007, Blanket Agreement Number: CNSHQ09A0021 (Page 7), executed on 11/23/2013.

[16] These controls include the inability of users to modify settings or to install any software; these changes must be processed through OIT.

vulnerabilities were being checked for,[17] but did schedule monthly vulnerability scans. The Deputy CIO explained to Kearney that because the Corporation selected and procured the MVM vulnerability scanning tool, the Corporation took responsibility for the monthly vulnerability scanning in an effort to reduce costs that would have been due under the terms of the MDCS. However, the Corporation did not provide any evidence showing that both the Corporation and MDCS contractor agreed to remove the contractual requirement for monthly vulnerability scanning in exchange for a fee reduction. The exercise of Option Year 4 of the MDCS contract on November 23, 2013 continued to include a requirement to maintain the security of the Corporation's network and follow NIST guidance for vulnerability scanning.

In addition, the Corporation did not correctly configure their new Multi-Protocol Label Switching (MPLS) network to allow network traffic from the MVM vulnerability scanner to communicate with the Corporation's field desktops. Further, the Corporation's Windows 7 firewall, installed on all desktops, was not correctly configured to accept network traffic from the MVM vulnerability scanner. Due to these configuration errors, the Corporation was unable to scan its desktops on a monthly basis.

Observation 2 – The Corporation received monthly vulnerability scan results from the MDCS contractor for scans of servers. Starting with the results for October 2013,[18] 39 high-risk vulnerabilities were identified.[19] These same 39 high-risk vulnerabilities were included with vulnerability scans each month from October 2013 through May 2014, indicating that neither the Corporation Information Assurance professionals nor the MDCS contractor reviewed the vulnerability report and took action to correct the 39 high-risk security weaknesses. In August 2014, Kearney reported the 39 high-risk security vulnerabilities to the Deputy CIO. He immediately took action, and informed Kearney that 24 of the 39 high-risk security vulnerabilities were remediated within 24 hours.[20] Ten additional risks were remediated within five business days of notification, and six additional risks will be mitigated by a change that was in the process of being rolled out, leaving only two risks remaining for mitigation.

Observation 3 – While the Corporation did not, in practice, conduct vulnerability scans of work stations, the Corporation conducted a scan upon Kearney's request for a sample of work stations located at headquarters.[21] Prior to the vulnerability scan's execution, the Corporation acknowledged that their desktops utilized vulnerable versions of Microsoft Internet Explorer and Java to maintain compatibility with the eSPAN. The results of the vulnerability scan did not identify missing application security patches or out-of-date software application software, such as Microsoft Office, Internet Explorer, Java, Adobe Flash, or Adobe Reader, on desktops known to be running vulnerable versions of software. The

[17] The current version of MVM was used to conduct the monthly scans; however, a review of the specific vulnerabilities being checked for was not conducted. While McAfee has predefined vulnerability sets, the Corporation should conduct a review of the checks to ensure the monitoring needs are still met.

[18] This is the first month for which evidence was received; these vulnerabilities may have previously existed.

[19] The 39 high-risk vulnerabilities were identified on servers to include Windows Domain Controllers, the MVM, the session initiation/voice over internet protocol (VoIP), asset management, VMWare, and VCenter management servers.

[20] Several of the risks mitigated within 24 hours were mitigated by powering off servers that were no longer being used, applying security patches to Windows Domain Controls, and altering security configurations.

[21] The Corporation's practice is to scan servers, not work stations. For the scan of work stations that Kearney requested, work stations at regional field sites could not be scanned due to the configuration settings of the MDCS network.

Corporation used the same level of scan configurations (i.e., non-intrusive Window operating system checks) as it used for Windows servers. The omission of these known vulnerabilities from the scan reports on work stations indicated that the Corporation's selected vulnerability scanning tool was not correctly configured to identify and alert the Corporation to all known security vulnerabilities on servers. While the vulnerabilities that would be identified for scans of work stations and servers may be different, if the tool did not identify commonly known vulnerabilities on work stations, the tool may also be prone to miss vulnerabilities on servers.

Observation 4 – The software version of the Corporation's vulnerability scanning tool, MVM, was not compliant with NIST vulnerability standards and did not support the Security Content Automation Protocol (SCAP). As a result, the Corporation was unable to independently confirm and demonstrate that its desktops were securely configured to the USGCB standard version 1.2,[22] as required by the MDCS contract.

Observation 5 – The Corporation had not established performance metrics or provided guidance to its MDCS contractor for the timely remediation of identified weaknesses.

Effect: Without conducting periodic and thorough vulnerability scans of both servers and desktops, the Corporation may not identify missing application and operating system patches. In addition, the Corporation may not identify significant configuration errors. The untimely remediation of vulnerabilities based on severity or risk can leave Corporation's network susceptible to malicious attack, possibly resulting in a breach of sensitive data and personally identifiable information (PII).

Vulnerability scanning is a critical control and tool for the Corporation to monitor the security of its network and confirms that the MDCS contractor adequately maintains the security posture of the Corporation's network. By not establishing and tracking performance against predetermined timeframes based on severity or risk, the Corporation does not know if its vulnerability management processes are effective, timely, focused on the areas of greatest risk, and its IT contractors comply with contractual terms.

[22] USGCB is a secure configuration standard for Windows XP, Vista, and Windows 7 desktop that specifies over 550 secure settings that NIST maintains and updates in response to new security vulnerabilities. The large number of security settings means that manual review is impractical without the use of an automated tool that supports the SCAP protocol.

Recommendation: Kearney recommends that the Corporation:

4. 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;
5. Include performance metrics[23] for vulnerability management in future MDCS contracts;
6. Update the MPLS network's configuration and Windows desktop firewalls to allow the Corporation's vulnerability scanning tool(s) to successfully communicate;
7. Test work station performance during intrusive scans to determine the feasibility of obtaining comprehensive vulnerability scan results;
8. Periodically perform scans of desktops and laptops using the current USGCB template from NIST to ensure ongoing compliance;
9. Upgrade or replace the Corporation's vulnerability scanning tool to overcome existing limitations and inaccurate scan results;
10. Implement a monthly process to review vulnerability scan configurations to include new vulnerability checks prior to scan execution;
11. Ensure that an appropriately configured vulnerability scan is conducted monthly against all information system components, including servers, routers, desktops, network printers, scanners, and copiers; and
12. Strengthen oversight of the Corporation's IT contractors to ensure vulnerability scan results are complete and reviewed, and identified weaknesses are remediated in a timely manner based on risk.

Finding #3: Organizational Conflict of Interest
(*See Appendix E, related DHS Question # 1: Continuous Monitoring Management)*

Background: FISMA requires agencies to conduct "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, of which such testing—(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory."[24] Building on the FISMA legislation, the NIST established the requirement that assessment of security controls be conducted by an impartial and objective party as the test results are relied upon by Federal officials to authorize an information system for operation in the Security Assessment and Authorization (SA&A)[25] step.

[23] Examples of performances metrics include the time to remediate and the number of vulnerabilities by risk level.
[24] 44 United States Code (U.S.C.) § 3544(b)(5)
[25] The SA&A process was previously known as Certification and Accreditation (C&A).

The Corporation entered into a five-year, fixed price contract with a MDCS provider (contractor).[26] The statement of work (SOW) issued with the blanket purchase agreement (BPA) contract stated:

> The Contractor is responsible for obtaining C&A and annual security testing of the hosted systems in accordance with NIST standards and CNCS[27] [Corporation for National and Community Service] policies, and providing documentation of these activities to CNCS. Certification and testing shall be performed or validated by an independent party and at MDCS contractor's expense.

In FY 2010, the MDCS contractor observed the above clause and contracted for an independent third party to perform the security assessment for the Corporation's LAN/WAN at its own expense.

The Corporation will use the results of this testing process to issue an Authority to Operate (ATO) for the GSS LAN/WAN and be the primary step in the SA&A process. The outputs of an SA&A process are an updated SSP, a Security Assessment Report (SAR), and updated Plans of Actions and Milestones (POA&M). In the performance of an SA&A, a security control assessor compares the control descriptions and implementation details from the SSP against the provider's actual security practices. Control failures are recorded in the SAR and uncorrected security weaknesses are recorded in the POA&M.

Condition: Under the supervision of the Corporation's Chief Information Security Officer (CISO), the MDCS contractor performed the SA&A of the Corporation's GSS in May 2013 and of eSPAN[28] in November 2013. Kearney identified that the resulting SSP, SAR, and POA&Ms contained multiple factual errors, inconsistencies, and omission of information that called into question the objectivity and rigor of the security assessment for the LAN/WAN and eSPAN. These errors also question the level of oversight and review of SA&A deliverables by the Corporation. For example, the security assessors, who also held network security monitoring responsibilities, used an obsolete and unsupported security tool from Cisco daily, but failed to record this weakness in their SAR or POA&M. Further, the LAN/WAN SSP indicated that the Corporation was using Internet Protocol Security (IPsec) protocol for virtual private network (VPN) connections, when the Corporation had deployed Secure Socket Layer (SSL)/Transport Layer Security (TLS)[29] VPN clients to its laptops several years before.

In addition, Kearney noted an inherent organizational conflict of interest in the use of the same MDCS contractor to both provide network, server, and desktop services and to perform security assessments over the same system. Under the terms of the contract, the contractor was paid a monthly fixed fee to deliver IT services to the Corporation. If the contractor's security assessors identify security weaknesses, the contractor would need to expend additional resources to correct these weaknesses by deploying additional

[26] The scope of services comprise managing the Corporation's GSS, including the LAN/WAN, Windows servers, Oracle databases, e-mail, VoIP phones, disaster recovery capability, network file share services, and other application support. As part of the MDCS contract, the contractor agreed to maintain a current "C&A"[26] of the GSS LAN/WAN.
[27] The Corporation is also known as CNCS, the Corporation for National and Community Service.
[28] eSPAN includes the eGrants application and My AmeriCorps Portal. eSPAN also has inherited a significant number of controls from the GSS, the common controls.
[29] SSL/TLS is encryption protocol for secure communications over the internet.

personnel or tools, such as a replacement for the Cisco Monitoring, Analysis, and Response System (MARS) tool,[30] to mitigate noted weaknesses. Correction of noted weaknesses would likely require additional expenditures without additional compensation from the Corporation due to the fixed price nature of the contract.[31]

Further, Kearney noted that the security assessment team reported to the same project manager as the network and server administrators, and not an independent party. As a result, the lack of additional compensating controls and project reporting structure would discourage the security assessors from identifying and self-reporting such weaknesses to the Corporation. The inherent weakness of this process is further exacerbated by the Corporation not providing effective oversight over the security assessment process, as evidenced by the factual inaccuracies in SSPs.

The organizational conflict of interest situation still continues, as the MDCS contractor performs the annual testing of one-third of NIST SP 800-53 security control tests for the GSS LAN/WAN.

Criteria: For information systems with a FIPS 199 moderate impact rating, NIST requires that security assessments be conducted by an independent assessment team in security control CA-2 (1) Security Assessments | Independent Assessor. NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, specifically states:

> Independent assessors or assessment teams are individuals or groups who conduct impartial assessments of organizational information systems. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the organizational information systems under assessment or to the determination of security control effectiveness. To achieve impartiality, assessors should not: (i) create a mutual or conflicting interest with the organizations where the assessments are being conducted; (ii) assess their own work.

Cause: The Corporation removed the contractual provision[32] contained in the SOW of the BPA requiring that the MDCS contractor procure an independent SA&A of the GSS and eSPAN major application. The Corporation stated that a contractual requirement for an independent SA&A was not contained in the performance work statement (PWS) for the third option year task order (TO). Thus, the MDCS contractor performed the SA&A. Regardless, oversight of the 2013 GSS and eSPAN security assessments did not identify multiple security weaknesses and shortcomings with the quality of the SA&A. As a result, there was a systemic failure of the SA&A process due to a lack of adequate checks and balances.

[30] Cisco announced end-of-life for MARS tool in May 2008, ceased maintenance support (i.e., patches) on November 30, 2011, and all technical support on November 30, 2013. It needs to be replaced as it is the Corporation's primary continuous monitoring tool.

[31] The MDCS contract, Statement of Objectives, v3.0, dated November 22, 2011, states, "Technology Refreshment and Replenishment - includes modernizing the IT infrastructure (both hardware and software) on a continual basis to ensure that infrastructure and system components stay current with evolving industry standards and technology platforms." The CNCS Contracting Officer's Representative (COR) awarded Option Year 4 with the above language on November 27, 2013.

[32] This provision is included in the SOW of the BPA and referenced in several contract modifications, including those that were effective after the SA&A process. Most recently, reference to the BPA SOW (Version 3.0, dated November 22, 2011) was reaffirmed November 27, 2013 with the exercise of the fourth option year.

Effect: The Corporation's decision to use the same contractor to perform information systems support as well as to identify security weaknesses over the same system it managed is an organizational conflict of interest that negatively impacted the SA&A process to provide impartial and objective results for the Corporation's GSS LAN/WAN. Lack of effective Corporation oversight limited the usefulness of SA&A results as a method to identify security weaknesses. Consequently, the Corporation may not be aware of security vulnerabilities and threats affecting its GSS, and thus not take timely actions to mitigate risk.

Recommendation: Kearney recommends that the Corporation:

13. 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;
14. Ensure that the Contracting Officer's Representative (COR) enforces all provisions contained within contracts, or a formal contract modification is to explicitly account for changes issued through the Contracting Officer (CO); and
15. Strengthen oversight of the Corporation's IT contractors to ensure implementation of the SA&A process complies with Federal standards.

Finding #4: Use of an Obsolete and Unsupported Network Tool
(*See DHS Question # 1: Continuous Monitoring Management)*

Background: MARS is a network appliance-based solution that provides network monitoring capabilities and collects audit logs from Cisco routers, switches, and Windows servers. Based on pre-defined security events and established e-mail distribution lists, the MARS tool analyzes the consolidated audit logs and can generate e-mail alerts in near-real-time to responsible individuals for further investigation. The Corporation's MDCS contractor utilizes the MARS tool to monitor the Corporation's network for unauthorized desktops, laptops, network printers, or other devices and alert appropriate individuals if an unauthorized network device is detected.

Per NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*:

> Automated tools are often able to recognize patterns and relationships that may escape the notice of human analysts, especially when the analysis is performed on large volumes of data… how effective the organization is in utilizing the monitoring results depends upon the organizational ISCM strategy, including validity and comprehensiveness of the metrics, as well as the processes in place to analyze monitoring results and respond to findings.

According to NIST SP 800-92, *Guide to Computer Security Log Management*, organizations should develop standard processes for performing log management, including log generation, transmission, storage, analysis, and disposal. Records should be stored with sufficient detail for a sufficient period of time to allow analysis of events. Routine log reviews and analysis are beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems shortly after they have occurred, and for providing information useful for resolving such problems, as well as identifying operational trends

and long-term problems. According to the National Archives and Records Administration's (NARA) General Schedule, *Chapter 8 Information Technology - Section 817 IT Security*, security audit logs should be retained for 12 months.

Condition: The Corporation's primary tool for network monitoring and audit log analysis is 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 IT vendor[33] did not replace the tool.

Additionally:

- The Corporation did not have a standard operating procedure requiring the periodic review and maintenance of the primary network monitoring and audit log tool, MARS. In addition, the MARS system administrator had not reviewed and tuned the audit alerts in more than two years;
- The MARS tool is unable to retain audit events online for more than two months. As a result, the usefulness of aggregated event logs to identify trends and perform targeted analysis is limited; and
- The Corporation 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.

[33] The Corporation uses a contractor to provide a GSS LAN/WAN.

Criteria: According to NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*:

> Automation serves to augment the security processes conducted by security professionals within an organization and may reduce the amount of time a security professional must spend on doing redundant tasks, thereby increasing the amount of time the trained professional may spend on tasks requiring human cognition. … The focus of an ISCM strategy is to provide adequate information about security control effectiveness and organizational security status allowing organizational officials to make informed, timely security risk management decisions. Thus, implementation, effectiveness, and adequacy of all security controls are monitored along with organizational security status.

According to NIST SP 800-92, *Guide to Computer Security Log Management*, organizations should establish and maintain successful log management activities, including standard processes for performing log management, with log management activities including log generation, transmission, storage, analysis, and disposal. Records should be stored in sufficient detail for an appropriate period of time. As part of the log management process, the organization should:

- Monitor the logging status of all log sources;
- Monitor log rotation and archival processes;
- Check for upgrades and patches to logging software, and acquire, test, and deploy them;
- Ensure that each logging host's clock is synced to a common time source;
- Reconfigure logging, as needed, based on policy changes, technology changes, and other factors; and
- Document and report anomalies in log settings, configurations, and processes.

Cause: The Corporation was not providing adequate contract oversight and had not developed a comprehensive process for network monitoring. The Corporation's contract with the MDCS contractor included a hardware refresh requirement.[34] However, the Corporation did not exercise its contractual rights and request that the GSS contractor replace the MARS tool prior to the product's End-of-Life (EOL),[35] and continued to use the tool. In addition, the contract did not include performance metrics for the timely remediation of identified vulnerabilities. In response to the noted observation, the Corporation's CIO indicated they accepted the risk to use an unsupported tool, Cisco MARS, as an evaluation of potential replacement tools did not provide the same functionality as Cisco MARS. However, this risk acceptance was not documented in the SSP for the GSS, the April 2013 SAR, or POA&M.

Effect: Use of an outdated network monitoring and audit log tool, as well as the lack of a periodic review of configuration settings, negatively impacts the Corporation's ability to monitor its information systems, leaving vulnerabilities unidentified for further analysis and remediation. Further, the limited data storage

[34] Specifically, the contract states that part of the requirement "includes modernizing the IT infrastructure (both hardware and software) on a continual basis to ensure that infrastructure and system components stay current with evolving industry standards and technology platforms."

[35] Cisco announced the "End-of-Life" on May 5, 2008 and the Corporation and the GSS contractor did not identify and implement a replacement tool before support ended on November 30, 2011.

capability of the MARS network appliance restricts the Corporation's ability to identify trends, which could help in identifying and remediating potential threats to its information systems and sensitive data.

Recommendation: Kearney recommends that the Corporation:

16. Identify and implement a replacement tool for network monitoring and audit log analysis to regain vendor software and hardware support;
17. 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;
18. Ensure IT contracts include clauses requiring contractors to only utilize tools that have both software and hardware support (as applicable);
19. 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;
20. Ensure network monitoring and audit log software can archive audit logs while still observing NARA's 12-month retention requirement for security audit logs; and
21. Develop and implement performance metrics to increase accountability for network monitoring and audit log review; improve effectiveness of information security; demonstrate compliance with Corporation policy, laws, and regulations; and identify areas for improvement.

2. Configuration Management

Finding #5: Lack of Controls to Prevent Use of Unauthorized Devices

(*See Appendix E, related DHS Question #2: Configuration Management)*

Background: The NIST SP 800-111, *Guide to Storage Encryption Technologies for End-User Devices*, states that in today's computing environment, there are many threats to the confidentiality of information stored on end-user devices, such as personal computers, consumer devices (e.g., personal digital assistant, smart phone), and removable storage media (e.g., Universal Serial Bus [USB] flash drive, memory card, external hard drive, writeable compact disk [CD] or digital video disk [DVD]). Some threats are unintentional (e.g., human error), while others are intentional. A common threat against end-user devices is device loss or theft. Malware, another common threat, can give attackers unauthorized access to a device, transfer information from the device to an attacker's system, and perform other actions that jeopardize the confidentiality of the information on a device.

Many threats against end-user devices could cause information stored on the devices to be accessed by unauthorized parties. To prevent such disclosures of information, particularly of PII and other sensitive data, the information needs to be secured. The primary security controls for restricting access to sensitive information stored on end-user devices are encryption and authentication. Centralized management is recommended for most storage encryption deployments because of its effectiveness and efficiency for policy verification and enforcement, key management, authenticator management, data recovery, and other management tasks.

Condition: The Corporation did not implement IT security policies and supporting technical controls to prevent the use of non-Corporation-issued portable data storage devices (e.g., USB thumb drives, external

USB hard drives, smart phones, and tablets). Further, Kearney observed Corporation employees utilizing personal devices for work purposes even though the Corporation did not have a bring-your-own-device (BYOD) policy that permitted such behavior. Corporation management stated that personal devices were only utilized for note-taking purposes, no different than a paper pad, were never configured to connect to the network, and were not authorized to contain any PII. Although the Corporation indicated that it had a policy regarding BYOD, Kearney's review of the employee's rules of behavior, the Corporation's IAP, and security plan for the GSS did not identify any policy regarding the use of personal devices for business purposes.

The Corporation's Rules of Behavior require that every individual with access to the Corporation network sign the following: "I will use 'encrypted' removable storage media (e.g., USB drives, portable hard drives, memory cards) to transfer PII or sensitive information. All sensitive data and PII transferred inside and outside the Corporation must be encrypted." However, the Corporation does not require employees and contractors to use only agency-issued storage media nor to use only federally approved cryptographic algorithms[36] to store PII. The Rules of Behavior imply that it is appropriate and acceptable for employees to use personal devices, such as USB storage devices, smart phones, and tablets, and connect these USB devices to the Corporation's IT resources, provided that they did not store sensitive information or the devices were encrypted.

In response to the noted observation, OIT management stated that a policy requiring Corporation-issued portable storage devices to be encrypted was issued. Corporation management further stated that the agency accepted the risk for employees to use personal devices by implementing policy and Rules of Behavior prohibiting storage of PII or other sensitive information on non-encrypted devices. However, the risk acceptance was not documented and Corporation devices were not forced to be encrypted through automated controls.

Criteria: OMB M-06-16, *Protection of Sensitive Agency Information*, requires all Federal agencies to take the following action:

> Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing.

[36] For non-national security systems, NIST establishes mandatory cryptographic algorithms that Federal agencies must use. These instructions are published in FIPS PUB 140-2, *Security Requirements for Cryptographic Modules.*

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, AC-19 (5), *Access Control for Mobile Devices | Full Device/Container-Based Encryption*, states:

> The organization employs [Selection: full-device encryption; container encryption][37] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].[38]

Cause: The Corporation did not establish a clear policy on the use and storage of sensitive information on personal devices and communicate this policy to all employees, members, and volunteers. Thus, Corporation employees, members, and volunteers freely use USB thumb drives, smart phones, tablets, and other personal devices for conducting official Corporation business.

Regarding the protection of sensitive information and the use of encryption, the Corporation did not communicate to employees whether the Corporation's encryption solution may be deployed on personal devices or offer other available alternatives. In discussions with Corporation IT management, they noted that users should contact the OIT Help Desk if they wished to use a portable data storage device. Finally, the Corporation has not enabled technical security controls on Corporation computers, such as forcing encryption on USB storage devices or preventing the computer from loading the software drivers to enable USB storage devices. The Corporation has implemented Windows BitLocker, which has the ability to fully encrypt USB drives; however, this solution is not compatible with Apple iPhones and iPads. Corporation management suggested that they are currently exploring options to encrypt some external storage devices and will determine implementation based on an assessment of risk and cost-effectiveness.

Effect: Without clear, enforced IT security policies regarding the use of personal devices for corporate use, Corporation employees and contractors may connect personal USB storage devices to Corporation computers and unknowingly introduce malicious software. Further, without additional guidance, employees and contractors may store sensitive corporate information on USB devices without encryption or sufficiently strong encryption algorithms. Finally, without adequate technical controls to force encryption on USB storage devices or block the use of unapproved USB storage devices, the Corporation may not be adequately protecting sensitive data from unauthorized use, access, disclosure, or sharing, thus elevating the risk of a data breach.

Recommendation: Kearney recommends that the Corporation:

22. Clarify and enforce the policy on the use of personal devices and USB storage devices for Corporation business and specify any required security controls or use restrictions; Clarification should include differentiation between personal BYOD and Corporation-issued devices;
23. Monitor the use of USB storage devices connected to Corporation computers and evaluate the risks presented by their use; and

[37] The Corporation has implemented container protection according to the GSS SSP.
[38] The Corporation defines this as "government furnished."

24. Complete the implementation of automatic encryption, included in the rollout of Microsoft Office 365, for portable data storage devices for user groups who regularly handle sensitive information (e.g., Procurement, Human Resources, and IT).

Finding #6: Risks to the Confidentiality of Voice Communications
(*See DHS Question # 2: Configuration Management)*

Background: The transmission of voice over packet-switched internet protocol (IP) networks introduces both opportunities and security risks. VoIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. Lower cost and greater flexibility are among the driving forces behind VoIP for the enterprise, but VoIP should not be implemented without careful consideration of the network architecture, risk tolerance, and inherent security issues that VoIP introduces.

The greater flexibility provided by VoIP phones creates multiple security weaknesses as the phones are configured dynamically when powered on. VoIP phones receive their configuration dynamically using an insecure, clear text protocol, trivial file transfer protocol (TFTP), from a central server called a Session Initiation Protocol (SIP) server or VoIP private branch exchange (PBX).[39] In most VoIP installations, there is no authentication between the Call Manager and the VoIP phone and dynamic configuration occurs based on the VoIP phone's unique network identifier, called a media access control (MAC) address. Other settings such as IP address, address of router, and other software specific settings for VoIP calls are dynamically configured, meaning intruders have a wide array of potentially vulnerable points to attack (e.g., phone, router, Call Manager, and multiple protocols). In contrast to legacy hardwired telephone systems, the dynamic nature of VoIP phone systems makes it more vulnerable to eavesdropping on conversations through data interception[40] and denial of service attacks. While confidentiality may not be the highest concern for some Federal organizations, availability and quality of service tend to be paramount as organizations rely upon their phone system for emergency 911 phone calls. For these reasons, the security and network design of VoIP are of paramount importance.

The NIST SP 800-58, *Security Considerations for Voice Over IP Systems,* offers Federal agencies nine recommendations to secure VoIP communications. The first of nine recommendations is "develop appropriate network architecture … separate voice and data on logically different networks if feasible."

[39] Call Manager is the term used by Cisco for the SIP Server or VoIP PBX and will be used going forward to represent the SIP Server or VoIP PBX.
[40] Most VoIP phone systems use either the H.323 protocol or the SIP for voice communication. Neither protocol uses encryption to protect the confidentiality of the voice conversation.

Condition: Kearney noted that the Corporation does not separate its data network traffic from its voice network traffic. Specifically, Corporation desktops were able to ping (query) Cisco VoIP phones at remote offices.[41] In addition, users were able to access the Cisco VoIP phones using their desktop's web browser over hypertext transfer protocol (HTTP).

Criteria: Because VoIP systems may be connected to the data network and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system. In SP 800-58, *Security Considerations for Voice Over IP Systems*, NIST offers nine recommendations to Federal agencies for securing the VoIP phone systems and states:

1. **Develop appropriate network architecture.**

   - Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate dynamic host control protocol (DHCP) servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection.
   - At the voice gateway, which interfaces with the [public switched telephone network] PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component.

Cause: The Corporation's contractor has not restricted access to the VoIP virtual local area network (VLAN); thus, desktops on data VLANs can communicate with VoIP VLANs. According to the Deputy CIO, the Corporation previously utilized a Cisco desktop application to configure and manage their VoIP phones; however, this desktop application is no longer used and the communication between the data VLAN and voice VLAN is not required.

The Deputy CIO expressed his concern that separating the VoIP and data VLAN would double the infrastructure costs. While true with first-generation Cisco VoIP equipment, current Cisco operating systems for routers and switches have a separate VLAN built in by default for the Cisco IP phones; thus, there is not a need to duplicate or have physically separate router and switch hardware for IP phones, as this can now be done virtually in software. Corporation management stated it was aware of the outdated architecture and contends that the VoIP and data VLANs are logically separated and secure.

Although the Corporation was aware and has accepted the risk of commingling voice and data traffic, the Corporation did not conduct periodic vulnerability scanning of its desktops or other IP VLANs outside of its server network segments, which may have identified additional vulnerabilities. Further, the May 2014 System Security Plan (SSP) for the LAN/WAN specifically stated that network traffic was limited on the VoIP VLAN. However, Kearney's observations and review of available evidence did not identify any limitation or restrictions between the data and voice networks. Finally, the Corporation has not recently

[41] NIST 800-58 notes that discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks.

contracted for a network penetration test to evaluate the attackers' ability to compromise or intercept phone conversations.

Effect: Connecting the data VLAN with the voice VLAN exposes the VoIP infrastructure to multiple attack vectors and security weaknesses. Knowledgeable individuals on the Corporation's data network could use the connectivity between the data and voice VLANs to compromise VoIP components, which generally were not designed with security in mind. For example, the use of unencrypted voice protocols and weak authentication between VoIP phones and the Call Manager could allow an attacker to intercept and record phone calls without the knowledge of the caller by using a network protocol capture utility and a man-in-the-middle attack approach. NIST SP 800-58 identifies several other common network vulnerabilities with VoIP systems:

- Voice switch default password vulnerabilities;
- Wiretap vulnerability created by using a network protocol capture utility like WireShark or VoIPHopper;
- Address Resolution Protocol (ARP) Cache Poisoning and ARP Flood attack;
- Web Server Interface vulnerabilities on phone and Call Manager;
- IP Phone Netmask Vulnerability (i.e., "man-in-the-middle attack");
- DHCP Server Insertion Attack;
- TFTP Server Insertion Attack; and
- Exploitable software flaws in Call Manager software.

Finally, attacks against the VoIP infrastructure would likely go undetected as the Corporation uses an obsolete network monitoring tool[42] and does not regularly review the audit logs of the Cisco Call Manager.

Recommendation: Kearney recommends that the Corporation:

25. 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;
26. 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;
27. Consider contracting for a network penetration study and including the Corporation's voice network within the scope of the study;
28. Determine if the legacy Cisco desktop application is still needed and remove it from all desktops and laptops if determined to be unnecessary; and
29. 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.

[42] Please refer to Finding #4: *Use of an Obsolete and Unsupported Network Tool*.

3. Identity and Access Management

Finding #7: Lack of Segregation of Duties
(*See Appendix E, related DHS Question # 3: Identity and Access Management)*

Background: Effective segregation of duties (SoD) starts with sound entity-wide policies and procedures implemented at the system and application levels. Responsibilities should be segregated so that one individual does not control all critical stages of a process. Entity-wide policies outlining the responsibilities of groups and related individuals pertaining to incompatible activities should be documented, communicated, and enforced. Failure to limit user access and processing capabilities to job descriptions that are consistent with compatible functions may result in errors in accounting records.

Condition: Kearney noted that the Corporation did not meet SoD compliance guidance as set forth by the NIST and OMB. Specifically, Kearney noted that the Corporation's management did not complete documentation of where SoDs must exist. The Corporation's POA&M, dated June 2, 2014, states, "Request Senior Management Support to identify a business sponsor(s) and initiate a project to address the segregation of duties finding in the eSPAN system…" and has a milestone date of to be determined (TBD). This is the same information that was provided in the FY 2013 FISMA evaluation and the same finding first reported in the FY 2011 financial statement audit. In the past four years, the Corporation has not demonstrated meaningful progress to resolve a longstanding weakness, despite indicating they are in the process of completing an assessment to define the required SoDs across all business processes, and align this with its IT systems, including eSPAN. eSPAN includes the eGrants application and My AmeriCorps Portal.

Criteria: NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Section AC-5, "Separation of Duties," states:

> Control: The organization:
> - Separates [*Assignment: organization-defined duties of individuals*];
> - Documents separation of duties of individuals; and
> - Defines information system access authorizations to support separation of duties.
>
> Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

OMB Circular A-123, *Management's Responsibility for Internal Control*, Section II, "Standards," states:

> Control activities include policies, procedures and mechanisms in place to help ensure that agency objectives are met. Several examples include: proper segregation of duties (separate personnel with authority to authorize a transaction, process the transaction, and review the transaction); physical

controls over assets (limited access to inventories or equipment); proper authorization; and appropriate documentation and access to that documentation.

Cause: Corporation management has not prioritized the establishment of a SoD matrix for eSPAN and devoted resources to designing and implementing SoD within eSPAN. Based on discussions with the CISO and Deputy Director of Program Coordination, the Corporation has started, but has not yet completed, the development of an SoD Matrix for the eSPAN application system, including access control policy and associated access controls.

Kearney observed that the Corporation has created a matrix for the GSS and the Momentum financial system. The Corporation also has implemented a quarterly review process overseen by the Deputy CIO to check for irregularities of all users and the roles to which they are assigned.

Effect: If users are provided excessive privileges or incompatible functions within eSPAN, eGrants, or My AmeriCorps Portal, there is an increased risk that erroneous or fraudulent transactions could be processed without being detected in a timely manner. Without properly defining roles that must be segregated and documenting how and where the system enforces proper segregation of duties (roles), the risk of improper transactions increases. Further, access-related controls, such as the review of a user's access provisions/privileges in eSPAN, eGrants, or My AmeriCorps Portal, may be ineffective due to inaccurate review criteria.

Recommendation: Kearney recommends that the Corporation:

30. Strengthen its controls surrounding SoD by documenting and maintaining an SoD Matrix for eSPAN that identifies the incompatible roles within the system. Specifically, the business process owners should work with the OIT to prioritize development of the SoD Matrix to identify where SoD violations could occur and restrict access accordingly.

4. Incident Response and Reporting

Finding #8: Inadequate Incident Response Reporting

(See Appendix E, related DHS Question #04 Incident Response and Reporting)

Background: NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, states, "incident response has become necessary because attacks frequently cause the compromise of personal and business data." Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. Further, FISMA requires the OMB Director to establish a Federal information security incident center to "compile and analyze information about incidents that threaten information security."[43] Accordingly, DHS established the United States-Computer Emergency Readiness Team (US-CERT), a Government-wide incident response organization that assists Federal civilian agencies in their incident handling efforts, and serves as a focal point for dealing with incidents. Federal agencies should follow incident response instructions and associated reporting timelines published by US-CERT.

Condition: The Corporation has not properly classified all computer security incidents and, as a result, has not reported all computer security incidents to the US-CERT, including:

- Three lost laptops, a Category 1 event; and
- Three instances where a Corporation user shared his/her user ID and password with another Corporation employee, a Category 4 event.

Criteria: The US-CERT analyzes the agency-reported security incidents to identify trends and indicators of attacks. These trends are easier to discern when reviewing data from many organizations than when reviewing the data of a single organization. For reporting incidents, US-CERT established six Federal Agency Incident Categories to improve communications among, and between, agencies:

1. CAT 1 – Unauthorized Access,
2. CAT 2 – Denial of Service,
3. CAT 3 – Malicious Code,
4. CAT 4 – Improper Usage,
5. CAT 5 – Scans/Probes/Attempted Access, and
6. CAT 6 – Investigation.

Exhibit 2 presents the category, description, and required timeframes for reporting the two categories of computer security incidents that the Corporation did not report.

[43] 44 U.S.C. § 3546(a)(2)

Exhibit 2: Federal Agency Incident Categories

Category	Name	Description	Reporting Timeframe
CAT-1	Unauthorized Access	An individual gains logical or physical access without permission to a Federal agency network, system, application, data, or other resource.	Within one (1) hour of discovery/ detection.
CAT-4	Improper Usage	A person violates acceptable computing use policies.	Weekly

NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, defines a computer security incident as "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." To assist in incident handling, NIST SP 800-61, Revision 2, also identifies attack vectors which can be used as a basis for defining more specific handling procedures.[44] Theft and improper use are both reportable incidents in accordance with the NIST guidance. While an agency may have some latitude in reporting events to the public,[45] there is no such latitude in reporting events to US-CERT.

Cause: The Corporation's Security Incident Log noted that three Corporation laptops were reported lost during FY 2014. In each case, the CISO required that the employee file a police report for the stolen/lost laptop. However, the incidents were not reported to the US-CERT based on the rationale that employees know not to store PII on their laptops and the laptop hard drives are encrypted. However, according to US-CERT criteria, loss of laptops constitutes a security incident as a person gains unauthorized physical access without permission.

The Security Incident Log also noted three instances where an employees shared their user identification (ID) and passwords with another Corporation employee. According to the CISO, the three incidents were not reported to the US-CERT, as the offending employee either locked another employee's network account or had the same network privileges and security profile as the individual who lent their user ID and password. Therefore, the CISO did not consider any of the three instances of a shared user ID and password a "security incident." Under US-CERT criteria, sharing an employee's user ID and associated password is a violation of acceptable computing use policies and must be reported as a computer security incident.

[44] NIST SP 800-61, Revision 2, specifically includes, "**Improper Usage,** which is any incident resulting from violation of an organization's acceptable usage policies by an authorized user,", "… and; **Loss or Theft of Equipment**, which is "the loss or theft of a computing device or media used by the organization, such as a laptop, smartphone, or authentication token."

[45] As discussed in OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, the factors that give discretion in reporting to the public "do not apply to an agency's notification to US-CERT."

The current CISO introduced the requirement to file a police report, thus enhancing the documentation requirements and evidence for some incidents. However, the Corporation did not recognize the potential for harm and, therefore, did not comply with the required standards for reporting security incidents to US-CERT.

Effect: The Corporation did not comply with Federal standards for reporting computer security incidents to the US-CERT and support US-CERT with their data-gathering responsibilities.

Recommendation: Kearney recommends that the Corporation:

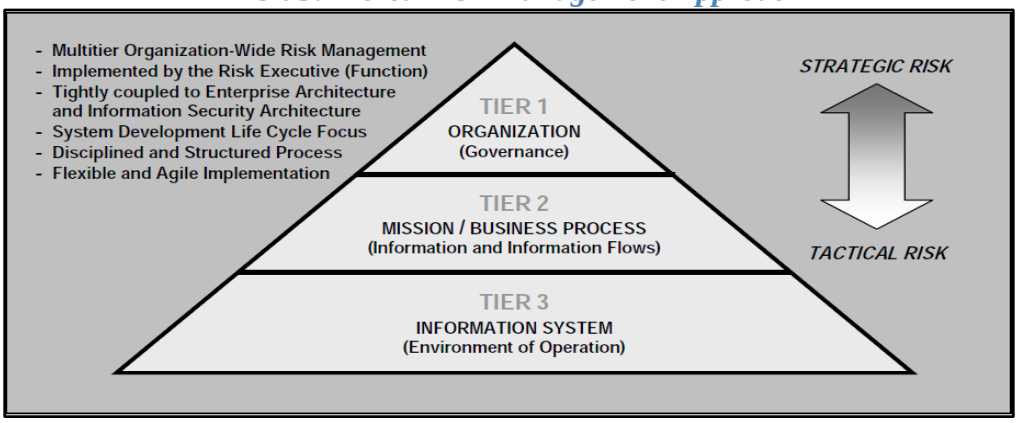
31. Update the Corporation's Incident Response Plan to align with NIST SP 800-61, *Computer Security Incident Handling Guide*, and US-CERT guidance to properly classify and report computer security incidents; and
32. Report all required security incidents to the US-CERT within the mandatory timelines.

5. Risk Management

Finding #9: Inadequate Enterprise-Wide Risk Management Policies and Practices
(*See DHS Question #05: Risk Management)*

Background: NIST SP 800-39 *Managing Information Security Risk: Organization, Mission and Information System View*, directs Federal agencies to integrate IT security risks into three tier levels in descending order: Tier 1 (Organization), Tier 2 (Mission/Business Process), and Tier 3 (Information Systems). Results of the risk management process ultimately feed into the Capital Planning and Investment Control (CPIC) process.

Exhibit 3: Tiered Risk Management Approach[46]



[46] Exhibit from NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*

Tier 1 addresses risk from an organizational perspective, providing the context for all risk management activities carried out by the Corporation. Tier 1 risk management activities directly affect the activities carried out at Tiers 2 and 3, including a prioritization of missions/business functions at the Tier 2 level, and the allocation and deployment of management, operational, and technical security controls at the Tier 3 level. Tier 1 decisions also drive investment strategies and funding decisions, thus affecting the development of enterprise architecture.

Tier 2 addresses risk from a mission/business process perspective and is driven by the risk context, risk decisions, and risk activities at Tier 1. Tier 2 activities directly affect the activities carried out at Tier 3.[47] For example, enterprise architecture decisions at Tier 2 affect the design of information systems at Tier 3, including the types of information technologies acceptable for use in developing those systems. The activities carried out at Tier 2 can also provide useful feedback to Tier 1, possibly resulting in revisions to the organizational risk frame or affecting risk management activities carried out at Tier 1.

Tier 3 addresses risk from an information system perspective and is guided by the risk context, risk decisions, and risk activities at Tiers 1 and 2.[48] At Tier 3, information system owners, common control providers, system and security engineers, and ISSOs make risk-based decisions regarding the implementation, operation, and monitoring of organizational information systems. In addition, the activities at Tier 3 provide essential feedback to Tiers 1 and 2.

Condition: Kearney noted that the Corporation documented its risk management policies and security controls in its IAP and in the respective SSP for its GSS and major applications[49] (MA). However, these documents described the risk management process at the information system (Tier 3) level and discussed specific technical, management, and operational security controls focused at that level. Existing risk management processes do not address risks at Tier 1 and Tier 2, and largely do not involve the business owner or application owner.[50] Examples where business owners should be extensively involved in risk management processes but were not include the development of business impact analysis (BIA)[51] for the

[47] Tier 2 level risk management activities include: (i) defining the mission/business processes needed to support the missions and business functions of the Corporation; (ii) prioritizing the mission/business processes with respect to the strategic goals and objectives of the Corporation; (iii) 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 Corporation; (iv) incorporating information security requirements into the mission/business processes; and (v) establishing an enterprise architecture with embedded information security architecture that promotes cost-effective and efficient IT solutions consistent with the strategic goals and objectives of the Corporation and measures of performance.

[48] Tier 3 risk management activities include: (i) categorizing organizational information systems; (ii) 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 (iii) managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development life cycle process implemented across the organization.

[49] The Corporation has two major applications. Momentum, the Corporation's financial reporting system, and eSPAN. eSPAN includes the eGrants application and My AmeriCorps Portal.

[50] However, the Corporation noted the ERB sits at Tier 1 and contributes to the management of risk within the agency. However, the ERB charter indicates that the responsibilities of the ERB, as they relate to risk, are not sufficient to cover Tier 1 and Tier 2 risk management activities. The ERB charter did not address implementation or managing techniques.

[51] Please refer to Finding #14: *Inadequate DRP Documentation and Planning*.

Corporation's critical systems, testing of the Continuity of Operations Plan (COOP),[52] and regular review of POA&M.[53] While business process owners may be involved if they are assigned a role as a key participant[54] in the change request process, they are unlikely to be involved prior to that time. Risk decision processes should ultimately be enterprise-wide and integrated into the CPIC process.

Kearney reported that the Corporation lacked a comprehensive and enterprise-wide Risk Management Program in the FY 2013 FISMA evaluation; this issue included a lack of integration between the business owners and the OIT. The Corporation has not made any progress to address this issue in FY 2014.

Criteria: NIST provides specific guidance to Federal agencies for implementing risk management controls in two key NIST SPs, listed below:

- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*; and
- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, states:
  The objectives of an integrated, organization-wide view for managing risk include:
  - Ensuring that senior leaders/executives recognize the importance of managing information security risk and establish appropriate *governance* structures for managing such risk;
  - Ensuring that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
  - Fostering an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
  - Helping individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

[52] Please refer to Finding #15: *Lack of Adequate Testing of COOP*.
[53] Please refer to Finding #12: *Improvements Needed to POA&Ms*.
[54] Roles and responsibilities that would be considered a key participant include, Information System Security Manager (ISSM), ISSO, Information Owner (IO), Information System Owner (ISO), and Authorizing Official (AO).

NIST SP 800-39 further states:

> Risk management is a comprehensive process that requires organizations to: (i) *frame* risk (i.e., establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.
>
> Organizations identify external entities with which there is an actual or potential risk relationship (i.e., organizations which could impose risks on, transfer risks to, or communicate risks to other organizations, as well as those to which organizations could impose, transfer, or communicate risks). External risk relationships include, for example, suppliers, customers or served populations, mission/business partners, and/or service providers.

Cause: Several years ago, the Corporation made a conscious decision to outsource its GSS,[55] its major applications, and its external public facing websites to different commercial providers. Risk management planning primarily focuses on these service providers at the Tier 3 level. The Corporation has not, however, developed a comprehensive enterprise-wide risk management process to provide effective oversight for developing, implementing, and operating these individual systems in support of the Corporation's core missions and business processes.

The Corporation did not consider its risk management processes to be deficient and, therefore, made no improvements in FY 2014. According to OIT officials, the Corporation's current risk management process is effective and additional documentation evidencing its integration is unnecessary and would be wasteful. The Corporation stated that all system security assessments and decisions are made in the context of the business use of data and involvement of business process owners is incorporated by default. Corporation management stated that the agency maintains an adequate, enterprise-wide risk management framework that is risk-based and cost-effective and that risk-based and cost-effective measures do not inherently indicate weakness and increased risk.

However, Kearney noted multiple weaknesses in the Corporation's continuous monitoring and risk management processes at the information system level (Tier 3).

[55] The GSS for the Corporation is the LAN/WAN.

These weaknesses are reported separately in the following findings:

- Finding #1: *Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring Program*;
- Finding #2: *Multiple Weaknesses with Vulnerability Scanning and Remediation*;
- Finding #3: *Organizational Conflict of Interest with Security Assessment and Authorization*;
- Finding #4: *Use of an Obsolete and Unsupported Network Monitoring Tool;*
- Finding #10: *Weaknesses with the Corporation's Security Planning and Assessment Process*; and
- Finding #16: *Inadequate Controls over Privacy Data*.

Kearney noted other security weaknesses at Tier 2, such as the lack of current BIAs[56] for the Corporation's critical systems, inadequate testing of the COOP,[57] and regular review of POA&Ms by business owners. The large number of security control weaknesses at both the information system level (Tier 3) and business level (Tier 2) indicate that the Corporation's existing risk management practices were not effective. However, the Corporation asserted that its contingency planning was adequate, but may not be documented, and that the Corporation is on par with other best practices in the industry.

The Corporation has focused contingency efforts on the MDCS. While the MDCS is a vital part of the Corporation's COOP, there are other aspects of the Corporation's functions that warrant attention. Current contingency planning does not adequately account for the interdependence of many of these systems, such that failure of one system in an emergency situation may cause the COOP plan to fail, leaving the Corporation unable to restore operations.

The Corporation has not made meaningful progress implementing corrective actions to address the risk management activity deficiencies first reported in the FY 2013 FISMA report.

Effect: Collectively, multiple security weaknesses preclude effective risk management from the information system level (Tier 3) to the enterprise level (Tier 1). Further, the lack of a documented comprehensive Risk Management Program that includes Tiers 1, 2, and 3 undermines the Corporation's ability to address and mitigate the risk associated with the operation and use of information systems that support its missions and business functions. The Corporation is vulnerable because it may remain unaware of information security risks affecting its systems, programs, and data.

[56] Please refer to Finding #14: *Inadequate DRP Documentation and Planning*.
[57] Please refer to Finding #15: *Lack of Adequate Testing of COOP*.

Recommendation: To help ensure an integrated, organization-wide program for managing information security risk for its IT systems, Kearney recommends that the Corporation:

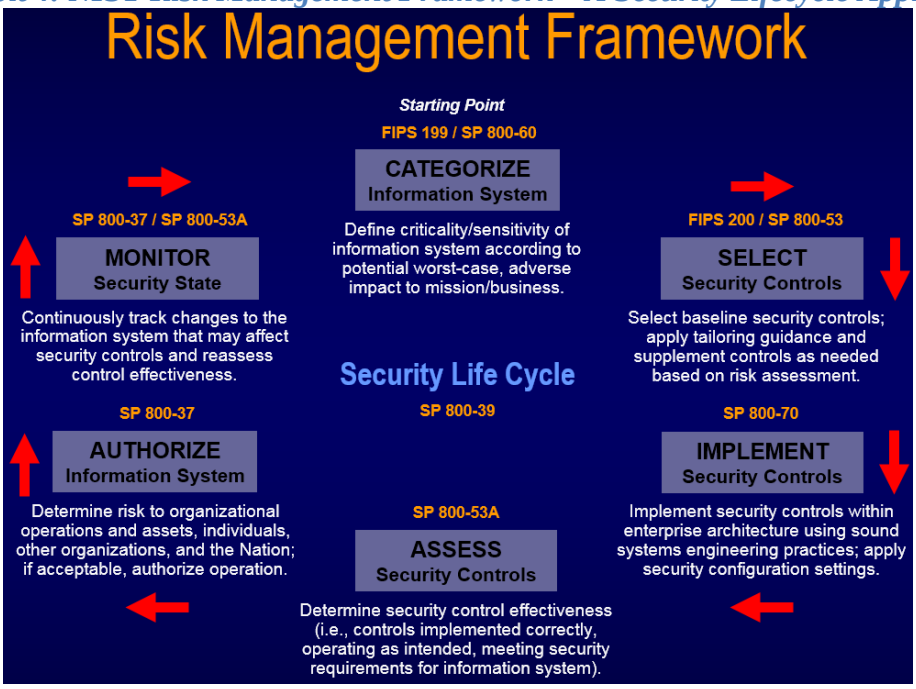
33. Document and fully implement a comprehensive and enterprise-wide risk management process, that includes the following:
    a. Addressing and capturing risk at the organizational level (Tier 1), providing the context for all risk management activities carried out by the Corporation in order to understand where risk resides for prioritization of remediation strategies;
    b. Addressing and capturing risk at the mission/business process level (Tier 2), including clearly assigning ownership and responsibilities for executing risk management processes at this level;
    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; and
    d. Integrating the risk management process with the CPIC process.

Finding #10: Weaknesses with the Corporation's Security Planning and Assessment Process
(*See DHS Question # 5: Risk Management)*

Background: In 2010, the Corporation developed a strategy to outsource its major information systems including its GSS,[58] financial application (Momentum), grants management system (eSPAN), and public-facing websites. In an effort to lower IT costs and improve service delivery, the Corporation awarded fixed-price contracts to each IT service provider. As part of each contract, the Corporation required the service providers to be compliant with FISMA and maintain the security of their respective information systems. This responsibility to be FISMA-compliant included activities such as preparing and maintaining SSPs and monitoring security controls effectiveness using guidance from the NIST and the associated NIST Risk Management Framework (RMF). The NIST RMF, shown below, presents a six-step approach for integrating information security and risk management into the traditional lifecycle of information systems.

[58] The Corporation's GSS includes the data center, the LAN/WAN, the VoIP, database server support, and desktop support.

Exhibit 4: NIST Risk Management Framework – A Security Lifecycle Approach



Source: Dr. Ron Ross, NIST, Computer Security Division, Presentation on May 21, 2013

Parallel to the IT outsourcing strategy in 2010, the Corporation partially shifted responsibility for information security to its IT vendors, but retained some operational securities responsibilities such as performing monthly vulnerability scans. Beginning in 2013, the IAP has transitioned from a security operations role to a security oversight function. Daily security functions such as monitoring the Corporation's firewalls, reviewing network audit events, managing end-user accounts, and implementing technical security controls became an IT vendor's tasks, rather than the Corporation's responsibility.

Condition: As part of the outsourcing strategy, the Corporation did not develop corporate standards for its multiple IT contractors to follow regarding ongoing security assessments and continuous monitoring activities. Kearney's testing of IT security controls across multiple Corporation information systems identified multiple inconsistencies and inaccuracies in the SSPs, SARs, and POA&Ms, highlighting the inconsistent nature, depth, and quality of security assessments and continuous monitoring activities performed by the Corporation's IT vendors. In addition, none of the eight POA&Ms identified programmatic security weaknesses with controls implemented by the Corporation rather the POA&Ms were generally limited to technical security control failures of the specific information system.[59] Kearney attributes these observations to a lack of clear and specific procedures and templates for contractors to conduct security assessments and continuous monitoring activities.

[59] Please refer to Finding #12: *Improvements Needed to Plan of Actions and Milestones*, for additional details.

While the Corporation has provided high-level guidance in its November 2012 IAP and the GSS LAN/WAN SSP, the Corporation did not provide detailed instructions to ensure consistency and compliance with NIST guidance when conducting security assessments. Specifically, Kearney observed:

- The Corporation has not developed standard test cases to capture evidence of control effectiveness, promote re-use of tailored test cases, and ensure consistency across security control assessments;
- The Corporation has not developed a sampling plan for testing the operating effectiveness of controls, thus limiting the comparability between subsequent assessments, such as comparing continuous monitoring results from 2013 to 2014;
- The Corporation has not documented its approach for testing common controls or how the Corporation assesses required security controls that are not within the scope of the IT service provider's information systems.[60] Examples include NIST SP 800-53 security controls that are frequently outside an IT vendor's responsibility and implemented at an entity level are *Security Awareness and Training, Incident Response, Personnel Security, System and Services Acquisition* and *Program Management*;
- The Corporation has not specified when security assessor independence and impartiality is required and when it may be waived. NIST requires independence for high and moderate impact systems; however, the Corporation has waived this requirement for its moderate impact systems, GSS LAN/WAN and eSPAN;
- The Corporation did not require its security control assessors to compare the implementation details from the SSP to actual practice and note any discrepancies. Hence, the SSPs for GSS LAN/WAN, eSPAN, and Momentum were not updated and accurate; and
- The Corporation has established templates for Acceptance of Risk that evidence the CIO and business owner sign-off on risk acceptance for security control failures that the Corporation elects not to remediate, but does not use them for all identified risks.

Criteria: FISMA legislation 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." NIST has developed guidance, SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for Federal agencies to follow (see ***Exhibit 4***). The RMF has a six-step process that culminates in Step 6, *Monitor Security Controls,* for information systems in operations. Rather than re-assessing all security controls every three years, Continuous Monitoring advocates assessing a subset (e.g., one-third of the NIST SP 800-53 security controls) on an annual basis to support the annual re-authorization of an information system.

When significant changes occur to an existing information system, such as a significant application upgrade, changes in the information system's primary data center, or changes in the information system's contractor, Federal agencies are required to repeat the six-step process outlined in the NIST RMF. Following a significant change to an information system, a key activity in the RMF is Step 2, *Select Security Controls*. Selecting security controls involves: (1) reviewing the mandatory 159 moderate impact NIST SP 800-53 security controls and the 26 privacy controls; (2) determining whether each control is

[60] The Corporation does not have a "common controls" security plan or a "privacy controls" security plan.

common,[61] hybrid,[62] or information system specific; and (3) allocating those controls to an organization or an information system. This is an important activity as it ensures accountability for each security control and avoids duplicating efforts by different security assessors retesting the same "common control." In SP 800-37, Revision 1, and SP 800-53, Revision 4, NIST encourages Federal organizations to develop "Common Control" security plans and "Privacy Control" plans to promote the idea of control assessment re-use and controls inheritance.

Once controls have been allocated to the organization or information system, Federal agencies should implement these security and privacy controls using NIST SP 800-53, Revision 4, in RMF Step 3, *Implement Security Controls*. In RMF Step 4, *Assess Security Controls*, Federal agencies select a security control assessor and develop and document a security assessment plan using guidance from NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.* Prior to executing the assessment plans, the Government official should approve the selection of security assessor, confirming appropriate independence exists, and review and formally approve the security assessment plan. Execution of the security assessment involves confirming the boundaries and scope of the assessment and evaluating the design and operating effectiveness of in-scope security and privacy controls based on the details in the SSP. At the completion of RMF Step 4, *Assess Security Controls*, the assessor prepares an SAR, records any outstanding control weaknesses on the POA&M, and updates the SSP to reflect observed implementation details and noted control failures.

In RMF Step 5, *Authorize Information System*, the information system owner (i.e., Authorizing Official) reviews the SAR, POA&M, and updated SSP to determine if risk is acceptable for the system to operate and formally accepts the risks and responsibility for information security by issuing an authorization decision, either ATO, interim-authority to operate (IATO) with restrictions, or denial. In RMF Step 6, *Monitor Security Controls*, the information system owner and ISSO implement the continuous monitoring plan for the information system and perform ongoing security control monitoring and periodic assessment using NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and NIST SP 800-53A.

Cause: Kearney identified four key reasons for the weaknesses with the information security control assessment process and inconsistencies in the scope, quality, and depth of the security assessment.

First, with the decision to outsource the Corporation's information systems to contractors, the Corporation did not prioritize the development of a security assessment approach supported by test cases, templates, and a quality assurance (oversight) process. Rather, each IT provider independently determined the depth, scope, and quality of testing for its information system. In addition, the strategy to outsource and put security assessment requirements with its IT providers overlooked contractual and budget realities. The Corporation's contractors are generally compensated on a monthly, fixed-price basis to deliver specific IT

[61] A common security control is inherited by one or more organizational information systems. Source: NIST SP 800-37, Revision 1
[62] A hybrid security control is implemented in an information system in part as a common control and in part as a system-specific control. Source: NIST SP 800-37, Revision 1

services. Each vendor has a motive to deliver the services at the lowest possible cost to achieve a profit. As a result, security assessments are often deemed to be an ancillary duty and security controls, such as SoD, costs money to implement and often conflict with the profit motive of the contractor. To mitigate this organizational conflict of interest, the Corporation did not exercise adequate oversight and review of their IT contractor's security assessment plan, sampling approach, and evidence of test results to confirm that completed testing was adequate in depth, scope, and quality. Further, the Corporation did not provide effective oversight, both in establishing specific information security standards for contractors handling critical IT functions and in ensuring that the contractors had effective programs in place to meet applicable Government-wide information security standards.

Second, the Corporation did not perform adequate planning in advance of their decision to outsource their IT systems. In particular, the Corporation did not closely review and update the assignment of responsibility for implementing each of the NIST SP 800-53 security controls and incorporate this assignment of responsibility in resulting contracts prior to their outsourcing. Instead, the Corporation grouped all its common and privacy NIST SP 800-53 security controls into a single SSP, the GSS LAN/WAN, rather than allocating the security and privacy controls to the Corporation, its MDCS contractor, or other IT contractors in accordance with NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. By placing all common security controls and system specific security controls in a single LAN/WAN SSP, responsibility for implementing each of the security controls was not clearly established. ***Exhibit 5*** illustrates how the Corporation could have allocated its security and privacy controls using NIST SP 800-37 guidance and differentiated between security controls primarily implemented by the Corporation and those security controls implemented by IT vendors.

Exhibit 5: Illustration of Control Allocation Concepts using NIST SP 800-37

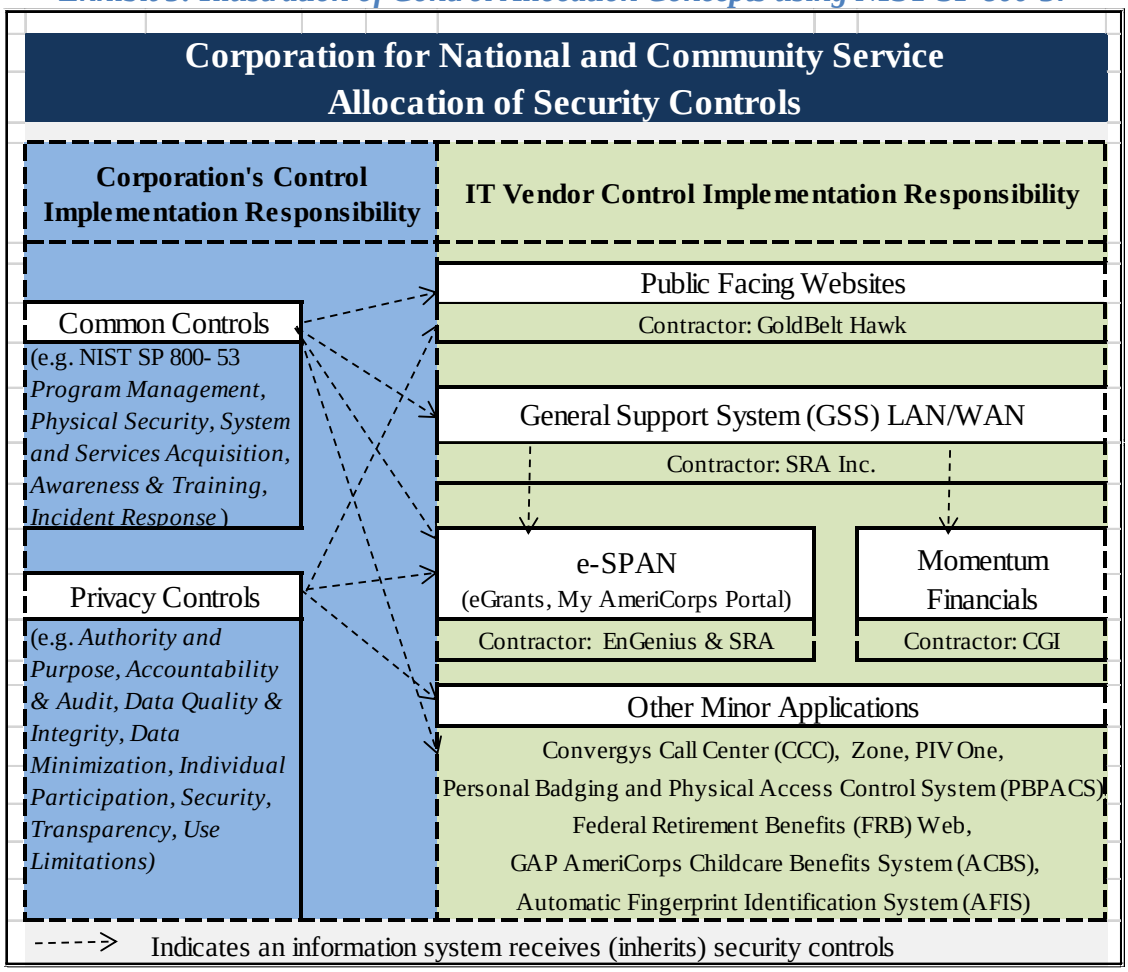


Exhibit 5 also illustrates how common controls and privacy controls are inherited by the Corporation's information systems, such as Public Facing Website, GSS LAN/WAN, eSPAN, and Momentum.

Third, according to the Deputy CIO, funding limitations prevented the transfer of certain IT security responsibilities to its MDCS contractor, such as regular maintenance and tuning of the Corporation's vulnerability scanner and network monitoring tool, Cisco MARS appliance. Omissions to the SARs and POA&Ms for LAN/WAN and eSPAN could be attributed to conflicting opinions between the MDCS contractor and Corporation on scope of the control assessment and ultimate ownership for implementing specific security controls and related security control enhancements.

Fourth, the Corporation has historically updated the SSP for each of its information systems every three years as part of the SA&A[63] process rather than on a continual or annual basis as required by NIST SP

[63] This process was formerly known as the C&A process.

800-37 and SP 800-53. The lack of adequate oversight and confirmation that its IT vendors annually updated the SSP after the completion of SA&A contributed to the outdated SSPs.

Further, the Corporation did not identify the organizational conflict of interest that resulted from expecting fixed-price contractors to identify problems in their own performance that would require additional work with no additional compensation.[64] The organizational conflict of interest increased the risk to the Corporation that security vulnerabilities would exist and not be reported. At a minimum, to mitigate the organizational conflict of interest, the Corporation should have increased oversight of the contractor; however, additional oversight did not occur and the Corporation did not detect inadequacies in the performance of security assessments, SARs, and POA&Ms.

Kearney noted in the FY 2013 FISMA report that the Corporation did not have an established process for monitoring selected security controls for information systems and that due to eSPAN upgrades, the SA&A for the system was delayed. Since the FY 2013 FISMA evaluation, the MDCS contractor conducted an SA&A on eSPAN (see Finding #3: *Organizational Conflict of Interest*); however, the Corporation has not established a formal agency- and contractor-wide process for monitoring selected security controls for information systems.

Effect: Lack of a structured approach for performing security control assessments by the Corporation's IT vendors resulted in inconsistent quality and depth of testing and test results of questionable value. Further the strategy of relying upon IT vendors to self-assess did not produce impartial or objective results, leading the Corporation to be uninformed of security weaknesses.

Examples of omission of information or security control failures that Kearney noted, in the eSPAN, Momentum, or LAN/WAN documentation included:

- SSPs contained multiple factual errors;[65]
- SSPs did not identify the system boundary or the technology components within the system boundary (i.e., servers, network appliances, and software versions);
- SSPs did not account for all security controls and security control enhancements. Specifically, the SSPs did not address how the Corporation satisfied the 16 program management controls and 26 privacy controls;
- The eSPAN SAR and POA&M did not identify a lack of application audit logs for essential audit functions, such as user account creations, account deletions, and account modifications; and
- The LAN/WAN SAR and POA&M did not identify that the Corporation used an obsolete and unsupported network monitoring tool, Cisco MARS, in addition to weaknesses with vulnerability scanning.

[64] See Finding #3: *Organizational Conflict of Interest*, for additional information.
[65] For example, the April 2014 LAN/WAN SSP incorrectly stated that the Corporation used an IPsec VPN and FIPS validated encryption modules. In reality, the VPN was a SSL/TLS VPN device and used non-FIPS validated encryption modules. The SSP also stated the Corporation used an older and currently obsolete software tool for applying security patches to desktops when a completely different software product was utilized.

Finally, the lack of adequate planning for security assessments resulted in incomplete security assessments. Since the security assessments were performed by IT vendors over their respective information systems, common controls implemented by the Corporation were not assessed such as the 16 program management controls and 26 privacy controls from NIST SP 800-53.

Ultimately, weaknesses with the security assessment process defeated the larger objective of informing business owners of security weaknesses in their information system and determining whether these risks presented an acceptable level of risk.

Recommendation: Kearney recommends that the Corporation:

34. Develop and implement a single security assessment process consistent with NIST SP 800-37, Revision 1, and NIST SP 800-53A for the Corporation's IT vendors to utilize;
35. Establish security assessment standards, to ensure consistency and quality, such as:
    a. Sampling plan,
    b. Standard test cases, and
    c. Determination of security assessor independence requirements
36. Review all NIST SP 800-53, Revision 4, security and privacy controls and allocate responsibility for implementing those controls to either the Corporation or IT vendor for existing IT contracts;
37. Assign responsibility for implementing specific NIST SP 800-53 security and privacy controls to either Corporation or the IT vendor prior to signing the contract. Incorporate the results of such analysis in the resulting IT contract to avoid ambiguity and subsequent vendor requests for a change order;
38. Create a "Common Controls" security plan and Privacy Controls security plan for the security controls for which the Corporation will retain responsibility;
39. Update the SSPs for eSPAN, Momentum, and LAN/WAN to ensure:
    a. SSP contains an accurate description of the information system and any sub-systems,
    b. SSP clearly identifies the information system boundaries and technologies utilized within the boundary,
    c. Responsibility for implementing each NIST SP 800-53 control is clearly delineated between the Corporation and IT vendor, and
    d. SSPs accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls and required control enhancements
40. Strengthen oversight of its IT contractors to ensure that:
    a. All the SSPs are updated, and accurate, at least annually, and
    b. Document its review of the SSP, SAR, and POA&M as part of the IT oversight process
41. 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;
42. Annually assess a subset of the Corporation's common controls and privacy controls; and
43. Complete Acceptance of Risk forms to formally evidence the CIO and business owner sign-off on risk acceptance. Electronically store the Acceptance of Risk in a central location so they may be readily searched during risk considerations.

6. Security Training

Finding #11: Lack of Formal Role-Based Training
(*See Appendix E, related DHS Question # 6: Security Training)*

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

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

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

Condition: NIST requires Federal organizations to provide role-based information security training to individuals with significant security responsibilities. In FY 2010, the Corporation self-identified this weakness and captured it on its POA&M.[66] As part of the FY 2013 FISMA evaluation, Kearney reported that the Corporation had not deployed a role-based security training program for all individuals with significant information security responsibilities. The Corporation responded to Kearney's FY 2013 FISMA finding by stating that it would "…provide better documentation of desk-side role-based training and may implement the draft generic role-based training modules if it can be determined to be an enhancement of the current training activities." The Corporation did not record this planned action on any of its POA&Ms.

In FY 2014, the Corporation gave, and offered evidence of, end-user awareness training, but only provided limited evidence of role-based training for certain individuals with significant information security responsibilities. While the Corporation's ISSOs and Information System Security Managers (ISSM) received additional training, other individuals with substantial IT responsibilities did not receive training commensurate with their job functions and responsibilities. These positions include:

- Corporation CIO,
- Corporation Senior Security Consultant,
- Corporation Project Manager,
- Momentum Data Center ISSO,
- Momentum ISO, and
- System Administrators (other than the GSS).

The Corporation's MDCS contractor provided "Security Awareness and Incident Handling" training to employees on how to maintain a secure environment and acknowledge security responsibilities. The training highlighted individual roles and their assigned duties in the event of an incident. Security training also involved explanations for reporting to the US-CERT for security incident category levels 0-6. However, training topics only covered awareness and were not specifically targeted to their job functions. IT contractors for the Corporation's two major applications,[67] Momentum and eSPAN, received no additional training beyond that provided by the Corporation. OIT management told Kearney that contractor personnel with access to agency systems and data were required to have appropriate security training but provided no documentation to support this assertion.

[66] This was recorded on the GSS POA&M in 2010 as FY10-NET22. Due to a numbering integrity issue, FY10-NET22 was closed and the issue was noted as being moved to FY10-NET110. However, FY10-NET110 was not included on either the Open or Closed portions of the GSS LAN/WAN POA&M.
[67] The Corporation has two major applications, Momentum, the Corporation's financial reporting system, and eSPAN, and its related subsystems.

Criteria: NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, distinguishes between Awareness and Training and specifically states:

> Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly… Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.
>
> * * *
>
> At the "Training" level of the learning continuum, the specific knowledge and skills acquired may become obsolete as technology changes.
>
> * * *
>
> "Awareness" constitutes the point-of-entry for all employees into the progression of IT security knowledge levels; the "Training" level, starting with "Security Basics and Literacy," then builds a wide range of security-related skills needed by employees in several functional area categories; and the "Education" level is the capstone of the learning continuum—creating expertise necessary for IT security specialists and professionals.

NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, Section AT-3, "Security Training," states:

> The organization provides role-based security-related training:
> - Before authorizing access to the system or performing assigned duties;
> - When required by system changes; and
> - [Assignment: organization-defined frequency][68] thereafter.
>
> **Supplemental Guidance**: … In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures.

Cause: The Corporation lacked a comprehensive role-based security training program. With few exceptions, its information security education for staff and contractors is limited to awareness; it did not provide or require continuous learning to maintain and update the skills of IT employees and contractors with significant information security responsibilities. The Corporation indicated that it provided one-on-

[68] According to its network SSP, the Corporation has defined an annual frequency for personnel with specific security-related functions and notes that specialized training is designed to assist with performance of security-related duties (e.g., ISSM and CISO).

one training to individuals who assumed new roles with significant information security responsibility; however, the Corporation did not maintain evidence of this training. Finally, the Corporation's oversight of its IT contractors was deficient in that it did not require them to demonstrate annually that their IT employees with significant information security responsibilities received security training relevant to their roles and responsibilities and technologies utilized.

The Corporation's CISO provided evidence of security training for some ISSOs and ISSMs as recommended as a result of the FY 2013 FISMA evaluation. However, review of the slides used as a template for the training showed this to be awareness, rather than skills and knowledge training. According to the Corporation, it is not financially feasible to provide role-based security training to the number of individuals with significant information security responsibilities. Further, it asserts that no annual training is necessary because its IT professionals each received training through their prior employment and education. Thus, it asserts that the limited awareness training provided by the CISO to most IT employees was suitable considering the size of the agency.

Kearney noted in the FY 2013 FISMA report that the Corporation had not documented and implemented a comprehensive role-based security program and that certain role-based security training modules were developed but were not yet approved and disseminated throughout the Corporation. Since the FY 2013 FISMA evaluation, the Corporation has made progress on this issue; however, the Corporation has not implemented all the necessary corrective actions to fully resolve this finding.

Effect: A strong IT security program cannot be implemented without significant attention given to educating the Corporation's IT users on security policies, procedures, and techniques. Because information security is dynamic, with new threats and vulnerabilities constantly developing, it is essential that all Corporation staff who manage the IT infrastructure and have significant information security responsibilities maintain current skills and knowledge commensurate with their job functions. Failure to give attention to security training puts the enterprise at great risk because security of Corporation's resources is as much a human issue as it is a technology issue. Without regular training, individuals with significant information security responsibilities may not keep abreast of new IT threats and vulnerabilities and the techniques to mitigate them.

Recommendation: Kearney recommends that the Corporation:

44. 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;
45. 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; and
46. Maintain evidence of security training for the Corporation's employees and IT contractors with significant information security responsibilities.

7. Plans of Actions and Milestones

Finding #12: Improvements Needed to Plan of Actions and Milestones Reporting
(See Appendix E, related DHS Question #7 Plan of Action and Milestones)

Background: OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, requires agencies to identify and report on deficiencies in their Information Security Program. A POA&M is a tool that identifies tasks that need to be accomplished. It details the required resources, milestones toward meeting the task, and scheduled completion dates for the milestones. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Because corrective actions to known security weaknesses may require additional resources, Federal agencies should integrate the POA&M management process into their CPIC process.

Condition: The Corporation does not have an adequate POA&M management process in place to ensure all known security weaknesses are recorded, resources identified, and adequately monitored to include timely resolution. The Corporation provided Kearney with eight separate POA&M spreadsheets that represented all outstanding POA&M items. The Corporation has multiple POA&Ms due to a strategic decision to outsource many IT functions, and each IT vendor is responsible for maintaining their own POA&M.

Although the Corporation has multiple POA&Ms, the combination of all POA&Ms provided an incomplete representation of all identified weaknesses. Weaknesses that were omitted from the eight POA&M spreadsheets include:

- Items relating to the Corporation as a whole, and not to a specific IT vendor;
- Items identified in an independent evaluation of agency-wide IT strategy, operations, and technology adoption;
- Items identified in FY 2013 Office of Inspector General (OIG) FISMA evaluation;
- Items that were considered low or moderate risk by OIT personnel;
- Items with risks for which specific actionable recommendations were not provided as part of the report;
- Non-technical security issues that were business process related such as ensuring that contractors comply with information security program requirements; and
- High-risk, technical vulnerabilities from monthly vulnerability scans that were outstanding over 30 days.

The Corporation's decentralized process for POA&M management does not prioritize corrective actions for the Corporation as a whole. POA&Ms are prioritized by the ISSM or the ISSO for each system.

Further, 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.[69] In the

[69] All but one of the Corporation's POA&Ms included high-level resource requirements, such as "Current Staff" or "Current Staff, Additional Staff as Needed;" however, none of the POA&Ms provided an estimate of man-hours to complete the noted milestone or estimated costs for contractor support or software tools.

FY 2013 FISMA evaluation, Kearney reported similar weaknesses associated with identifying required resources with the Corporation's POA&M management process. While the Corporation improved the POA&M management process to include the retention of evidence associated with POA&M closure, the revised process did not include identifying required resources.

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

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

OMB Memorandum M-02-01 further states:

> An agency should develop a separate POA&M for every program and system for which weaknesses were identified in the Security Act reports, as well as those discovered during other reviews including GAO [Government Accountability Office] audits, financial system audits, and critical infrastructure vulnerability assessments. Thus, the POA&Ms should either reflect consolidation with, or be accompanied by, other agency plans to correct security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments.

NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, PM 4 - Plans of Action and Milestones Process, states:

> The organization:
>
> a. Implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:
> b. Are developed and maintained;
> c. Document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation;
> d. Are reported in accordance with OMB FISMA reporting requirements; and
> e. Reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, states:

> Following identification of the prioritization criteria, corrective actions should be prioritized against the criteria on the basis of cost and impact, first at the enterprise level and then at the system level.

Cause: The Corporation's outsourcing strategy requires contractors to maintain POA&Ms for their respective information system. Thus, security weaknesses spanning across multiple information systems are not captured. This is exacerbated by the lack of a Corporation-wide cross-contractor POA&M. Additionally, the Corporation utilizes a Change Request/ticketing process to capture requested technical changes to an application's functionality rather than the POA&M spreadsheet by system. As a result of this process, the Corporation discusses POA&Ms weekly during the PCCB meetings. This meeting also serves for the Corporation to discuss the costs and benefits of remediation of certain POA&M items while the PCCB determines which changes will be implemented.

Additionally, the Corporation's POA&M guidance does not contain clear instructions for recording identified security weaknesses and associated resources required to complete each POA&M item. If a finding in a report did not result in a specific actionable recommendation, the Corporation did not include it on a POA&M; the Corporation did not consider the risks identified and determine its own recommendation to address the identified risk. Further, if the Corporation accepted the risk identified, the Corporation will not include it on the POA&M and not document acceptance of the risk. The policies and procedures for formally managing IT security weaknesses are limited to the high-level guidance provided in the IAP, which does not include detailed instructions for documenting POA&M items. Finally, the Corporation has not established performance metrics or practices to communicate outstanding POA&M items to the Corporation's Chief Executive Officer (CEO) or Chief Operating Officer (COO) to gain additional executive support to remediate known weaknesses.

Kearney noted in the FY 2013 FISMA report that the Corporation did not identify resource needs or provide adequate supporting evidence in the closure of POA&M items. In the current FY, the Corporation provided documentation evidencing POA&M closures, but did not document its resource needs. Thus, while the Corporation has made progress on this issue, it has not implemented all the necessary corrective actions to resolve this finding.

Effect: The Corporation's decentralized approach toward POA&M management has several negative effects with regard to risk management. Because the POA&Ms omit low to moderate weaknesses, as well as process-based and vulnerability-scan weaknesses, the Corporation's executives may not have a comprehensive picture of the security weaknesses impacting its IT environment. Further, weaknesses that individually carry only low or moderate risk may in the aggregate present risks that are far more serious. Moreover, under the current POA&M practices, significant process-based and vulnerability-scan weaknesses might never receive attention from the Corporation's executives and system owners. Finally, to make sound strategic decisions about enterprise-wide priorities and the allocation of resources, the Corporation's executives require a comprehensive understanding of all information security risks. Depriving them of this information threatens to distort their decision-making.

Recommendation: Kearney recommends that the Corporation:

47. Enhance the POA&M process to identify resources required for remediation either in the POA&M item or associated change request ticket;
48. Establish a Corporation-wide, Information Security Program POA&M to track security issues that are broader than a single information system such as findings from management studies like the MITRE report or annual OIG FISMA evaluations; as part of this process, the Corporation should

turn broad risks into recommendations that are actionable and able to be included and tracked on a POA&M;

49. Document acceptance of risk for items that will not be remediated, along with planned mitigating controls; and
50. Strengthen the POA&M management process by: (a) developing detailed instructions for documenting POA&M items, (b) formally assigning responsibility for tracking and regularly updating all POA&Ms, (c) including all known security weaknesses, containing low and moderate, and (d) establishing performance metrics or practices to communicate, semi-annually or annually, to the Corporation's CEO or COO on known security weaknesses and associated resource needs, to coincide with budget requests.

8. Remote Access Management

Finding #13: Inadequate Controls over Remote Access
(*See Appendix E, related DHS Question # 08: Remote Access Management)*

Background: Remote access is the ability of an organization's users to access its non-public computing resources from external locations other than the organization's facilities. Federal agencies typically provide employees with remote access using VPN technology to support an agency's telework program and business continuity and disaster recovery initiatives. In determining the controls related to remote access technologies, agencies should assume that remote access devices and networks contain hostile threats that will attempt to gain unauthorized access; as such, additional protection is needed.

OMB and NIST have established mandatory security controls to address the risks of connecting mobile devices across unsecure networks such as the internet. In Memorandum M-06-16, *Protection of Sensitive Agency Information*, OMB issued specific, mandatory security controls to all Federal agencies following the loss of a Department of Veterans Affairs (VA) laptop containing PII on 26.5 million veterans. One of the four security controls mandated in OMB M-06-16 was to "…allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access."

In addition, NIST requires that agencies utilize only FIPS-approved cryptographic algorithms in VPN solutions and implement two-factor authentication to the desktop and network in NIST SP 800-53, Revision 4, *Recommended Security Controls for Federal Information Systems and Organizations*, security control IA-2, *Identification and Authentication*, using Personal Identity Verification (PIV) credentials.[70] The Corporation, however, maintains that, as a small Government corporation, it is exempt from the requirement to utilize PIV credentials for logical access; accordingly, the Corporation has not implemented PIV cards for logical access. While the Corporation is exempt from the requirement, Kearney believes the implementation of strong authentication through the use of PIV cards is a good

[70] The rationale from NIST is that advances in computing power, the ability to crack passwords, and the wide availability of tools that can covertly gain access and secretly extract information from computers have rendered the traditional combination of user-ID and password obsolete and ineffective against modern threats.

business practice in light of the many publicized instances where user identifications and passwords were stolen by hackers at commercial and Federal organizations.

Condition: Corporation-issued laptops were configured to automatically connect to the Corporation's network through Cisco's "AnyConnect VPN" client. However, the automatic connection of the laptop to 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." Although the Corporation requires a digital certificate (which is stored on the laptop), along with a user ID and password, the implementation does not meet the required level of authentication and tamper-resistance as the mandated two-factor or multi-factor authentication,[71] since the digital certificate resides on the same laptop as the user ID and password. In addition, the digital certificate can be exported to other devices, and the Corporation has deployed the same digital certificate, rather than a unique digital certificate, for each laptop. According to the Corporation, it has configured the SSL/TLS VPN concentrator to evaluate specific desktop settings, such as the installation of antivirus software on the laptop. If the settings are not consistent with the required configurations, the connection is terminated. The Corporation considers this validation process to be an adequate compensating control for the use of a single digital certificate.

In addition, the Corporation incorrectly configured its VPN to permit the use of non-compliant, FIPS[72] encryption protocols, leaving[73] VPN sessions vulnerable to exploitation, such as "man-in-the-middle attacks." Kearney also noted that the Corporation's VPN client was susceptible to several SSL/TLS vulnerabilities. While Cisco had issued Open SSL Cryptographic Library patches in June 2014, the Corporation had not installed the patches for the SSL/TLS VPN client as of August 25, 2014, the date Kearney reviewed the system. OIT management stated that the particular version of software installed was configured so that it did not listen to connection requests, so that running the unpatched (vulnerable) version was not an issue unless the configuration was changed to allow the receipt of requests. Management further stated that, based on their assessment, the Corporation would accept the risk that the updates were not required. However, Kearney notes that, in general, it is prudent to install software patches since the vendor has determined a need to address vulnerabilities by announcing the availability of security patches.

Criteria: According to OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Federal agencies are required to "allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access" for access to all Federal information.[74]

[71] Multi-factor authentication is an approach to authentication that requires the presentation of two or more of the three independent authentication factors: 1) a knowledge factor ("something only the user knows"); 2) a possession factor ("something only the user has"); and/or 3) an inherence factor ("something only the user is"). Examples of possession factors include RSA Security tokens and PIV credentials.
[72] FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*
[73] RC4, SSL 3.0, and SSL 3.1/TLS 1.0[73]. RC4, SSL 3.0, and TLS 1.0 are widely used commercially, but have several technical flaws that can increase the risk of exploitation.
[74] OMB M-07-16 also requires encryption, time-out functionality, logging and verification, and issuance of understanding of responsibilities.

NIST provides specific guidance to Federal agencies for remote access in NIST SP 800-52, Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. Specifically:

- Section 3, Minimum Requirements for TLS Servers, subsection 3.1, Protocol Version Support, states, "TLS version 1.1 is required, at a minimum, in order to mitigate various attacks on version 1.0 of the TLS protocol. Support for TLS version 1.2 is strongly recommended"
- Section 3, Minimum Requirements for TLS Servers, subsection 3.3 Cryptographic Support, 3.3.1 Cipher Suites, 3.3.1.1.1 Algorithm Support, states, "RC4 is not an Approved algorithm."

Additionally, NIST SP 800-113, *Guide to SSL VPNs*, states, "because of the way that SSL was designed, SSL versions 3.0 and earlier do not conform to the requirements of FIPS 140-2."

Cause: During deployment of the current VPN software, the MDCS contractor did not adhere to NIST or FIPS configuration guidance for multi-factor authentication when deploying the Corporation's SSL/TLS VPN. Since the Corporation's remote access users wanted to seamlessly connect to the Corporation's network, OIT had configured Corporation laptops to automatically connect over the SSL/TLS VPN once the user successfully entered their Windows user ID and password and the digital certificate had been authenticated. While the Corporation maintains that the validation of the configuration is a second authentication factor, the digital certificate, user ID and password, and configuration check all take place on the same laptop, which does not meet OMB and NIST requirements for remote access.

In addition, Corporation oversight of the VPN deployment and the most recent May 2013 SA&A did not identify the use of non-approved FIPS-140-2 protocols or that the Corporation's deployed VPN solution was not patched to remediate the risks associated with the Heartbleed SSL and related SSL/TLS vulnerabilities with the Cisco VPN client. The Corporation has asserted that it accepted risk related to not installing these security patches for the Cisco SSL/TLS VPN client, but the decision is not documented and mitigating controls have not been put in place. Further, the Corporation was not aware that the MDCS contractor was using an SSL/TLS VPN client rather than the IPsec VPN client as stated in the LAN/WAN SSP.

Effect: The Corporation's remote access solution relies largely on its employees protecting the confidentiality of their user IDs and passwords; it does not provide a unique digital certificate to each employee to further ensure appropriate identification and authentication; and it leaves the password cached on the Windows desktop, where it could be captured or exploited. In addition, all controls reside with the same laptop and, therefore, do not leverage multi-factor authentication through the use of a hardware token or PIV card. Finally, the SSL/TLS VPN concentrator uses weak cryptographic algorithms. Unfortunately, attackers are increasingly successful at obtaining user IDs and passwords from victims' computers and have successfully exploited these weaknesses to steal large volumes of information (e.g., credit card numbers, Social Security numbers, or protected health information) from organizational databases.

Without timely installation of vendor patches, the Corporation is relying on its configuration setting (no listening mode) to preclude the Heartbleed and other SSL/TLS vulnerabilities on the VPN client. This configuration may not stop all attacks against a vulnerable SSL/TLS VPN client, and a successful attack

could potentially compromise the confidentiality, integrity, or availability of the Corporation's network. Finally, the Corporation collects significant amounts of PII from its members, and attackers could potentially exploit this information for financial gain. If a PII exploitation occurred, the Corporation could be liable for damages and required to offer credit monitoring and related fraud-protection services, similar to the VA's loss of PII concerning its affected members and employees.[75]

[75] In FY 2014, the VA OIG highlighted that such services cost $37.50 per affected individual.

Recommendation: To help mitigate the risks associated with remote access and client devices used for telework, Kearney recommends that the Corporation:

51. Review and update the configuration of the SSL/TLN VPN device to comply with FIPS 140-2 approved cryptographic algorithms (i.e., 3DES, AES-128, AES-256, and SHA-1) and TLS 1.2;
52. Implement a VPN solution that complies with OMB M-06-16 and NIST SP 800-53, Revision 4, mandatory security controls for Federal agencies, by using multifactor authentication; and
53. Strengthen oversight of MDCS contractors to ensure proper implementations of IT products and timely installation of vendor-supplied patches; as necessary, develop a formal, documented risk acceptance process, to include establishment of mitigating controls.

9. Contingency Planning

Finding #14: Inadequate Disaster Recovery Plan (DRP) Documentation and Planning
(*See Appendix E, related DHS Question # 9: Contingency Planning)*

Background: An information system contingency plan consists of management policies and procedures designed to maintain or restore business operations, including computer operations, in the event of emergencies, system failures, or disasters. The NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, states:

> Because information system resources are so essential to an organization's success, it is critical that identified services provided by these systems are able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered as quickly and effectively as possible following a service disruption.

The first step in developing effective contingency plans is performing a BIA, which identifies critical business processes, associated resource requirements, and recovery priorities.

Condition: The Corporation's disaster recovery documentation does not demonstrate consideration of all of the agencies' functions and missions. The BIA specifically states:

> It is not meant to address the following business functions:
>
> - Corporate communications,
> - Availability of experienced personnel,
> - Facility services,
> - Finance (including accounts payable [AP] and Payroll),
> - Human Resources (including Benefits, Employee Training, Personnel Security),
> - Grants management,
> - Program management,
> - Purchasing,
> - Regulatory affairs,

- System restoration procedures,
- Recovery Plan, and
- Disaster declaration procedures.

The BIA indicates that these business functions are covered in the COOP and the Corporation DRP. However, the COOP and DRP plans did not reference the BIA or the critical business functions listed above. Review of the COOP and DRP shows that roles and responsibilities for individuals involved with disaster recovery are included, but does not demonstrate how each of the functions listed above was considered by the business process owners in selecting the recovery timeframe and strategy. Further, the Corporation's DRP is written specifically for the MDCS and is not representative of the Corporation as a whole nor does it acknowledge other key IT contractors and systems. Based on the review of available BIAs, DRPs, and COOP documentation, the Corporation has a gap in the Corporation's COOP and consideration of critical business functions.

While the Corporation has documented some elements and results from its evaluation of the BIA in the "Essential Functions and Personnel Section" of its COOP, all essential business functions, as noted above, should be included as part of disaster recovery documentation, along with input from the business process owners.

Criteria: NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* states:

> The BIA is the first source for determining resiliency and contingency planning strategies. BIA results determine how critical the system is to the supported mission/business processes, what impact the loss of the system could have on the organization, and the system recovery time objective. The BIA results can help determine the type and frequency of backup, the need for redundancy or mirroring of data, and the type of alternate site needed to meet system recovery objectives.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* further states:

> The BIA is composed of the following three steps:
>
> i. **Determine mission/business processes and recovery criticality.** Mission/Business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum time that an organization can tolerate while still maintaining the mission;
> ii. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible; and
> iii. Identify **recovery priorities for system resources.** Based upon the results from the previous activities, system resources can be linked more clearly to critical mission/business processes and functions. Priority levels can be established for sequencing recovery activities and resources.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems,* also states, "results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the organization's COOP, Business Continuity Plans (BCP), and DRP."

Cause: The OIT has chosen to develop a comprehensive corporate BIA plan, rather than a BIA for each system. As a result, business process owners were not involved in the establishment of contingency planning documentation. Further, the Corporation has not included all business functions in its DRP. Additionally, the Corporation is relying on the MDCS DRP to cover the entire Corporation. However, the plan, which focuses on MDCS systems, does not encompass all critical business functions needed to provide an adequate COOP for the Corporation as a whole. The Corporation's COOP briefly addressed resumption of critical business processes; however, adequate information to implement restoration of those critical business functions was not included or sufficiently detailed.

Effect: The lack of BIAs for each critical system, including input from the business owner, negatively impacts the Corporation's ability to prioritize its systems and processes; therefore, criticality in returning information systems to operation may not be timely, cost-effective, or in the correct recovery sequence. Additionally, the Corporation may not have identified and planned for needs outside of IT in its COOP, such as alternate facilities, vital records, and communication.

Recommendation: Kearney recommends that the Corporation develop a more effective and comprehensive DRP and COOP by:

54. Developing an individual BIA for each critical system with participation from the business owner;
55. Determining information system recovery criticality, including allowable downtime and acceptable data loss based on business process needs;
56. Identifying outage impacts, resource requirements, and recovery priority for system resources;
57. Updating the DRP to cover the entire Corporation and other critical IT contractors and not just the MDCS; and
58. Updating the COOP based on revisions to the BIA and DRP.

Finding #15: Opportunities to Strengthen Continuity of Operations Planning and Testing
(*See Appendix E, related DHS Question # 9: Contingency Planning)*

Background: Should an event occur that disrupts an organization's ability to meet its mission, organizations need to have plans in place to bring mission-essential functions back to operation as soon as possible. The COOP provides procedures and guidance to sustain an organization's mission-essential functions at an alternate site. The COOP is supported by the DRP, which provides technical details for bringing mission-essential information systems back online, generally at an alternate location. Organizations often use the phrase "contingency planning" to refer to "disaster recovery planning," as discussed in the guidance below. At a high level, contingency planning is a subset of continuity planning that focuses on the technical aspects needed to implement continuity of operations. NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* states:

> Continuity and contingency planning are critical components of emergency management and organizational resilience but are often confused in their use. *Continuity planning* normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. *Contingency planning* normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency.

Because the Corporation utilizes the term DRP to refer to contingency planning, Kearney will use the term DRP to address the technical aspects of information system recovery.

Although documentation of both continuity of operations and DRPs are important, testing of those plans is equally important to validate assumptions, confirm viability of plans, and verify adequacy of technology. Without adequate testing and communication to employees, a COOP may not be ready when it is needed most.

The Corporation has defined its mission-essential functions by function in the agency-wide COOP documentation. Some of the essential functions include:

- Location and accounting for office staff;
- Delegation of authority, budget and appropriations;
- Approving new grants and monitoring current grantees;
- Paying grantees and ensuring access to the Payment Management System;
- Paying employees and members;
- Disbursing funds to the Field Financial Management Center;
- Adjusting hiring needs to include temporary, part-time, and emergency workers;
- Ensuring wide area network and voice over internet protocol connectivity;
- Ensuring access to systems;[76]

[76] The Corporation has determined that the GSS LAN/WAN, Momentum, and eSPAN are critical information systems that support mission-essential functions.

- Providing protective service and security risk assessments; and
- Coordinating with law enforcement.

The Corporation has conducted some planning activities and developed an agency-wide COOP,[77] a GSS DRP, and a financial system[78] contingency plan. In FY 2014, the Corporation performed limited DRP testing that included the Corporation's communications systems and eSPAN.[79]

Condition: The Corporation has not conducted adequate planning or testing of its COOP. The following aspects of the Corporation's COOP and DRPs make it inadequate.

The COOP does not include sufficient information to address all mission-essential functions and subordinate plans and details that would be necessary, should the plan ever need to be activated. The need to activate the COOP will be determined by the 11 members[80] of the COOP Executive Team (CET) "through conference calls, meetings, or other communications."

The Corporation has made assumptions that do not appear reasonable, should it be necessary to activate the COOP. These assumptions include:

- All vital records are available electronically for all mission-essential functions. This would include records such as personnel files, grant and contract files, member files, etc.;
- Employees have access to Corporation-issued laptops that would allow them to continue work once information systems have been brought back online. Based on observation of Corporation HQ, many employees still use desktop computers;
- Employees have up-to-date phone numbers for key personnel; and
- Evidence of annual COOP testing, including after-action reports, as required for mission- essential functions and the agency's financial system did not exist. Bad weather and snow on February 13, 2014 resulted in a large number of employees and contractors teleworking, but many were unable to connect remotely to the Corporation's network due to insufficient VPN licenses. While this specific issue may be resolved, it highlights that unforeseen technical issues may arise and prevent successful recovery without testing.

Criteria: NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* does not state the frequency with which an organization must test their Information System Contingency Plan (ISCP), but does state:

[77] Appendix B "COOP Test and Exercises," Testing Plan Section 2 (COOP Activation) and Section 3 (Information Systems and Records [IT] DRP) briefly describe the organization-wide recovery.
[78] Momentum is the Corporation's financial accounting system and is maintained and hosted by a contractor.
[79] eSPAN includes the following related subsystems eGrants Phase II, eGrants Classic, Member Portal, Staff Portal and Grantee Portal.
[80] The CET includes the following: Inspector General (IG), General Counsel, Deputy Chief of Staff and Operations, Field Liaison, External Affairs, Chief of Staff, CEO, CFO, Human Capital, and IT.

> 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. Test and exercise schedules should be stated in the ISCP policy statement.

NIST SP 800-34, Revision 1, further states:

> Leadership roles should include an ISCP Director, who has overall management responsibility for the plan, and an ISCP Coordinator, who is responsible to oversee recovery and reconstitution progress, initiate any needed escalations or awareness communications, and establish coordination with other recovery and reconstitution teams as appropriate.

The Corporation has determined that the frequency of its COOP and DRP testing should be annually, according to the COOP, Appendix B – COOP "Test and Exercises," Section 2 (COOP Activation), and Section 3 (Information Systems and Records [IT] DRP). The document also stated that the timeline may change as directed by the COOP Coordinator.

Additionally, NIST SP 800-39, *Managing Information System Risk*, discusses the importance of involving senior leaders and executives in risk decisions and planning. It states, "at Tier 1 [i.e., top organizational level], senior leaders/executives, in consultation and collaboration with the risk executive (function), define the organizational risk frame including the types of risk decisions (e.g., risk responses) supported, how and under what conditions risk is assessed to support those risk decisions." COOP is one of several risk management functions that senior executives should lead.

Cause: The Corporation has assigned the OIT with the responsibility of disaster recovery planning. This responsibility is an ancillary duty of the OIT. The responsibility for COOP was assigned to the CET, putting control under the purview of multiple individuals, as opposed to one central leadership position. While the COOP has appropriate inclusion of executive-level officials outside of the OIT whose primary responsibilities are on the Corporation's business functions, rather than the technological aspects, the number of individuals involved may lead to confusion in the event of required activation. One individual involved with executive leadership should ensure that the COOP adequately addresses mission-essential functions and possible risks, as recommended in the NIST guidance.

Management may not conduct contingency exercises for the benefit of learning and improvement, but rather to satisfy audit requirements; thus the importance of planning and testing the COOP is diminished.

The Momentum DRP reflects this sentiment and states:

- Conduct a Team Notification Exercise, and document for audit purposes, and
- Conduct a Team Walkthrough Exercise, and document for audit purposes.

Effect: The Corporation is not in compliance with NIST policy and its own policies and procedures to conduct annual testing of COOP Activation and the Information Systems and Records (IT) DRP. Ultimately, the Corporation may not be able to sustain and recover mission-essential functions following a disaster event without clear leadership, proper planning, and testing. Further, without adequate continuity and disaster recovery planning, the Corporation may not have the necessary people and assets in place to resume operations and cannot be assured that the COOP is reasonable, effective, and complete, and that all personnel are aware of their roles in the execution of the plan. As a result, the Corporation cannot be assured that mission-essential functions can be restored in a timely manner to support the Corporation's operations in the event of an emergency, disaster, or loss of information systems.

Recommendation: Kearney recommends that the Corporation:

59. Define a clear chain of command to clarify responsibilities and identify an ISCP Director to oversee Corporation-essential functions regarding the COOP;
60. Review the assumptions that are included in COOP documentation and ensure that the assumptions are valid and realistic;
61. Update the COOP documentation to ensure that all mission-essential functions are considered and have detailed plans for resumption of operations; and
62. Conduct a COOP test at least annually and capture lessons learned in a formal after-action report.

10. Privacy

Finding #16: Inadequate Controls over Privacy Data

Background: The Corporation celebrated its 20th anniversary and received recognition by the current President of the United States and three former Presidents of the United States. The ceremony kicked off the year of service for approximately 75,000 AmeriCorps members who will join over 900,000 AmeriCorps alumni. To fulfill its mission, the Corporation collects extensive PII from its members, employees, and volunteers.

The escalation of security breaches involving PII has contributed to the loss of millions of records over the past few years. The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable, should PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal laws such as the Privacy Act of 1974 and Section 208 of E-Gov.

The likelihood of harm caused by a breach involving PII is greatly reduced if a Federal agency or organization minimizes the amount of PII it uses, collects, and stores. For example, a Federal agency

should only request additional holdings of PII, or PII in a different format, if the PII is absolutely necessary. Also, Federal agencies should regularly review their holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission.

Condition: Kearney identified weaknesses in the Corporation's implementation of privacy controls. These weaknesses include the following:

- The Corporation has not explicitly documented its privacy controls, as required by Appendix J of NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[81] The privacy controls encompass eight families:
  - AP – Authority and Purpose,
  - AR – Accountability, Audit, and Risk Management,
  - DI – Data Quality and Integrity,
  - DM – Data Minimization and Retention,
  - IP – Individual Participation and Redress,
  - SE – Security,
  - TR – Transparency, and
  - UL – Use Limitation
- The Corporation has not fully documented its PII inventory, which should be used as a tool to minimize the use, collection, and retention of PII as well as to confirm security controls over collections of PII are adequate;
- The Corporation employees did not observe NARA Record Retention Schedule requirements for records containing PII and destroy these records when the record retention limit was met. Also, the Corporation's PII Reduction Plan was established to ensure that information collected by the Corporation about individuals was limited to that which is legally authorized and necessary and is maintained in a manner that protects against unwarranted intrusions upon individual privacy. In addition to not following NARA, the Corporation does not follow its own policy which states, "eliminate the retention of PII that is no longer needed." Kearney observed member files containing PII that was outside of the retention period at the Volunteers in Service to America (VISTA) Member Support Unit (VMSU) and at the North Central Region North Central Region National Civilian Community Corps (NCCC) offices; and
- Kearney reviewed the Privacy Impact Assessment (PIA) for two key information systems, Momentum and eSPAN, and noted that the PIAs for both systems have not been updated since 2009. Since the PIAs were created five years ago, the Corporation has implemented significant enhancements to eSPAN, established a data warehouse, undertaken IT modernization, and established additional information sharing agreements with other Federal agencies. These technology changes, functional enhancements, and additional uses of member data require the Corporation to inform the public. Currently, the Corporation does not publically post PIAs on its

[81] The privacy controls are based on the Fair Information Practice Principles (FIPP) embodied in the Privacy Act of 1974, Section 208 of E-Gov, and OMB policies. As stated in the NIST publication, the FIPPs are designed to build public trust in the privacy practices of organizations and to help organizations avoid tangible costs and intangible damages from privacy incidents. The privacy controls encompass eight families, each aligning with one of the FIPPs.

website. The Corporation has included a list of the PIA available with contact information to request a copy.

Criteria: The Privacy Act of 1974 was enacted "to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies… [to] collect, maintain, use, or disseminate any record of identifiable personal information … and that adequate safeguards are provided to prevent misuse of such information…" To provide the same protections to electronic information as those found in paper records, Section 208 of E-Gov established additional legal requirements for all Federal agencies, including the completion of a PIA. Among the many requirements, Section 208 encouraged Federal agencies to, "Each agency shall – …3. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency."

OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* establishes specific criteria when agencies must update their PIAs and identifies nine events such as significant systems changes and new interagency use.

The Code of Federal Regulations, 45 (45 CFR), Part 2508, Implementation of the Privacy Act of 1974, § 2508.10 (a)(2) states, "All records, when not under the personal control of the employees authorized to use the records, must be stored in a locked metal filing cabinet."

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, specifically requires agencies to:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete;
- Reduce PII holdings to the minimum necessary for proper performance of agency functions;
- Develop a schedule for periodic review of PII holdings; and
- Establish a plan to eliminate the unnecessary collection and use of social security numbers.

NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Section 4.1.1 Policy & Procedure Creation* states:

> Organizations should consider developing privacy policies and associated procedures for the following topics:
> - Access rules for PII within a system,
> - PII retention schedules and procedures,
> - PII incident response and data breach notification,
> - Privacy in the system development life cycle process,
> - Limitation of collection, disclosure, sharing, and use of PII, and
> - Consequences for failure to follow privacy rules of behavior.

NIST SP 800-53, Revision 4, was released in April 2013; therefore, this SP became mandatory of all Federal agencies in April of 2014, one year after the release date. NIST SP 800-53 states, "Federal agencies should begin implementation of these security controls by documenting their required security and privacy controls in either a 'Common Controls' or a Privacy Controls System Security Plan (SSP)."

Cause: Kearney observed that several factors contributed to the privacy weaknesses above.

The Corporation did not develop and require implementation of the required NIST SP 800-53, Appendix J: Privacy Controls. The Corporation has assigned the responsibility for privacy primarily to one individual, who is tasked with several other duties; thus, privacy is an ancillary duty.

In the current era of constrained OIT resources, the Corporation relies extensively on privacy practices developed in response to the FY 2010 privacy breach and has not updated these privacy practices to reflect guidance issued in April 2013 by NIST. The November 2012 IAP discusses privacy, but does not address the eight privacy control families or provide implementation details found in a Privacy Controls SSP. Generally, a perception that the November 2012 IAP is sufficient has prevented the Corporation from implementing a comprehensive Privacy Program.

In 2012, the Corporation developed an inventory of PII to assist the Corporation in complying with privacy control requirements to minimize the use, collection, and retention of PII. According to the Corporation's CISO, the OIT reviews and updates it annually. However, Kearney noted that key PII information was not consistently included for all PII items,[82] and thus limited the inventory's usefulness to minimize the use, collection, and retention of PII and as a tool to confirm adequate security protections were in place.

In addition, while it is the Corporation's policy to destroy or delete files containing PII when the records are no longer needed, Kearney observed that the VMSU and the North Central Region NCCC did not comply with the NARA record retention schedule and destroy physical records containing PII once the expiration date had passed.

Effect: Without comprehensive oversight and continuous monitoring of privacy controls for ongoing effectiveness, the Corporation may not be adequately protecting personal information from unauthorized use, access, disclosure, or sharing, thus elevating the risk of a privacy breach. Should a breach occur, the Corporation may be financially liable for costs of credit protection services that can be very large depending on the number of members affected by the breach. Using the 2013 Annual Financial Statement, the Corporation reported serving approximately 1.2 million members. According to publicly available information from the VA OIG, the cost of providing one year of credit monitoring and fraud protection services may range from $10 to $37.50 per affected individual, depending on fraud insurance limits. In a worst case scenario, such as a compromise of the eSPAN database, the cost of a breach could be between $12 million and $45 million for credit monitoring services and potentially more for related IT incident response and mitigation services.

Recommendation: To help ensure effective oversight of the Corporation's privacy controls, Kearney recommends that the Corporation:

[82] Kearney reviewed the tracking sheet and noted that the document includes an annual review, as well as dates of collection, confidentiality impact levels, how the PII is used, and other information to determine if a Privacy Threshold Analysis, a subsequent Privacy Impact Analysis, or System of Record Notice is needed.

63. Update, document, and implement the privacy controls required by Appendix J of NIST SP-800-53, Revision 4, and perform continuous monitoring as necessary to comply with the provisions of the publication;
64. Re-evaluate the sufficiency of resources to implement required privacy controls and ensure an individual is identified and assigned responsibility for these privacy controls;
65. Fully document information contained in the PII tracking sheet, as part of improving the process to minimize the use, collection, and retention of PII;
66. Ensure Corporation staff are aware of, and comply with, NARA retention requirements for maintaining physical PII records; and
67. 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 E-Gov.

APPENDIX B: STATUS OF PRIOR YEAR FINDINGS

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our" in this report) followed up on the status of the Notice of Findings and Recommendations (NFR) reported in the Federal Information Security Management Act of 2002 (FISMA) Independent Evaluation for fiscal year (FY) 2013, Office of Inspector General (OIG) Report 14-03. Through the testing procedures completed, Kearney determined the current status of the prior issues:

#	Previously Reported Finding	Auditor's Position on Status
1	**Subject:** Lack of a Formally Documented and Fully Implemented ISCM Strategy **Condition:** The Corporation has not formally documented and implemented an organization-wide ISCM strategy, as mandated by Office of Management and Budget (OMB) guidance and required by four National Institute of Standards and Technology (NIST) Special Publications (SP). The Corporation's Information Assurance Program (IAP) provides for the continuous monitoring of information system (Tier 3) controls; however, the IAP does not define all processes supporting a Continuous Monitoring Program across the entire organization or define meaningful, reportable metrics for all business processes supporting the Corporation's mission. **Recommendation:** Kearney recommends that the Corporation: 1. Document and fully implement an ISCM strategy that incorporates the following: a. Establishment of metrics to be monitored; b. Establishment of frequencies for monitoring/assessments; c. Ongoing security control assessments to determine the effectiveness of deployed security controls; d. Ongoing security status monitoring; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address the results of the analysis; and g. Reporting of the security status of the organization and information system to senior management officials consistent with guidance in NIST SP 800-137.	Sufficient corrective action has not been taken; see FY 2014 Finding #1: *Lack of a Formally Documented and Fully Implemented Information Security Continuous Monitoring (ISCM) Strategy*.

#	Previously Reported Finding	Auditor's Position on Status
2	**Subject:** Lack of Formally Documented and Fully Implemented Risk Management Framework (RMF) **Condition:** The Corporation's Risk Management Program addresses risk mainly at the information system (Tier 3) level. Policy and documented processes for system-level assessments were substantially compliant with requirements; however, Kearney noted the following: • The Corporation has not documented an organization-wide risk assessment that considers risks across the organization, including Tier 2 activities/business processes carried out by field offices; and • The Corporation did not annually assess the security controls or risks of its Electronic System for Programs, Agreements, and National Service (eSPAN) application. **Recommendation: Kearney recommends that the Corporation:** 1. Document and fully implement a process for addressing and capturing risk at the organizational/mission and business process levels throughout the organization; 2. Clearly assign ownership and responsibilities for executing risk management processes at the business/program level (Tier 2); and 3. Ensure compliance with processes for monitoring security controls at the information system level (i.e., Tier 3), and obtain formal approval and necessary waivers for departures from Corporation policy. Further, establish and communicate potential disciplinary actions for noncompliance with the Corporation's security policies.	Sufficient corrective action has not been taken; see FY 2014 Finding #9, *Inadequate Enterprise-wide Risk Management Policies and Practices*, and Finding #10: *Weaknesses with the Corporation's Security Planning and Assessment Process*.
3	**Subject:** Lack of a Fully Implemented of a Role-Based Information Security Training Program **Condition:** Although the FISMA legislation, OMB, and NIST require role-based security training for individuals with significant information security responsibilities, the Corporation has not documented and implemented a comprehensive role-based security program. Certain role-based security training modules have been developed, but have not yet been approved and disseminated throughout the Corporation. **Recommendation:** Kearney recommends that the	Sufficient corrective action has not been taken; see FY 2014 Finding #11: *Lack of Formal Role-Based Training*.

#	Previously Reported Finding	Auditor's Position on Status
	Corporation: 1. Implement role-based security training for all users with significant information security responsibilities.	
4	**Subject:** Improvements Needed to Plan of Actions and Milestones (POA&M) Reporting **Condition:** Kearney identified procedural weaknesses with the Corporation's management of POA&Ms: • POA&Ms did not clearly identify resources (man hours and/or costs) required to resolve open tasks; and • Supporting evidence for closing open POA&Ms was not consistently referenced and maintained in the Corporation's POA&M tracker. **Recommendation:** Kearney recommends that the Corporation: 1. Enhance the POA&M process to identify resources required for remediation either in the POA&M item or associated change request ticket; and 2. Strengthen the POA&M process to require individuals to reference evidence supporting the closure of a POA&M item.	Sufficient corrective action has been taken to address evidence for closing POA&Ms. Sufficient corrective action has not been taken for resource identification; see FY 2014 Finding #12: *Improvements Needed to POA&M Reporting*.
5	**Subject:** Improvements Needed to Ensure that Contractors Comply with the Corporation's Information Security Program Requirements **Condition:** Although the Corporation has defined general responsibilities for its Contracting Officers (CO), system owners, and IT support professionals to monitor its IT contractors, the Corporation does not have systems or processes in place to ensure that its employees actually provide the necessary oversight to confirm that contractors implement mandated security controls. Corporation guidance expressly requires the Corporation to ensure contractors, grantees, and other parties that operate information systems for the Corporation or handle data on the Corporation's behalf adhere to FISMA, OMB requirements, and the Corporation's information security and privacy policies. After reviewing IT contracts for the Corporation's Managed Data Center Services (MDCS) provider, its data center provider, and support services contracts for the eSPAN/My AmeriCorps Portal, together with the	Sufficient corrective action has not been taken. Kearney has included current year contractor compliance issues under the specific FISMA metric area to which the finding relates, rather than carrying forward this broad finding. See **Section 2.2 Information Technology Overview** for additional information.

#	Previously Reported Finding	Auditor's Position on Status
	procedures setting forth the relevant oversight activities, Kearney determined that the Corporation's process does not describe in sufficient detail the steps and evaluation criteria necessary for review of security assessment documentation (i.e., updated System Security Plan, Continuous Monitoring Plan, Contingency Plan test results, or updated POA&M) and security performance measures required from its IT contractors. Further, the IT contracts appeared to use a generic list of security requirements, but did not specify the security controls or a tailored set of security controls relevant to those contracted IT services. In addition, the IT contracts did not define information security goals and objectives, performance measures, and technical compliance requirements for measuring performance effectiveness, efficiency, or frequency of control execution. **Recommendation:** Kearney recommends that the Corporation: 1. Strengthen contractor oversight to ensure compliance with the Corporation's security requirements by clearly assigning oversight responsibility and required activities for COs, system owners, and supporting IT professionals.	
6	**Subject:** Lack of Two-Factor Authentication to the Corporation's Desktops, Laptops, and Corporate Network **Condition:** The Corporation's laptops and desktops have not been configured to use Personal Identity Verification (PIV) credentials for both physical and logical access control, as required by OMB Memoranda and NIST security guidance. **Recommendation:** Kearney recommends that the Corporation: 1. Research avenues to implement two-factor authentication, such as leveraging a Federal shared service provider to reduce upfront technology costs, lower per unit cost, and adopt a gradual, phased-deployment strategy to overcome current budget constraints.	Resolved the Corporation determined that its status as a Government corporation does not require it to implement PIV access controls. According to OMB, the Corporation is not required to implement two-factor authentication to the desktop; therefore, the issue was not repeated in FY 2014. However, the use of PIV is strongly recommended to provide enhanced security for remote access.

APPENDIX C: MANAGEMENT'S RESPONSE

Corporation for NATIONAL & COMMUNITY SERVICE
1201 New York Avenue, NW
Washington, DC 20525
202-606-5000
NationalService.gov

Tyler Harding, Principal Kearney and Company, P.C. 1701 Duke Street, Suite 500 Alexandria, VA 22314

October 22, 2014

Dear Mr. Harding:

The Corporation for National and Community Service (CNCS) appreciates the opportunity to review and comment on the draft report of Kearney and Company's Fiscal Year 2014 Federal Information Security Management Act (FISMA) Evaluation.

CNCS concurs with the conditions and recommendations reported in the draft report. We are committed to maintaining a strong and effective Information Assurance Program and protecting sensitive information in our systems. We are also committed to fulfilling our responsibility to the national service participants, grantees, and other stakeholders who trust us to protect the personally identifiable information they share with us.

While the draft report does not identify any actual breaches of sensitive information or personally identifiable information within CNCS's systems, it does identify risks and a pathway to improvement. The findings and recommendations in the evaluation report will be essential in improving our Information Assurance Program. We place a high priority on addressing these recommendations in a timely and effective manner.

To address the recommendations contained in the draft report, and to institute a sustainable Information Assurance Program, I am convening a FISMA Remediation Team. This team will report directly to the Chief Operating Officer and will address the four broad suggestions in the draft report to develop, document, and implement an agency-wide Information Assurance program to assure CNCS systems and data are protected.

In the short term, the team will address the recommendations about our FISMA

deficiencies based on the level of risk to agency operations. This team will also provide a longer-term plan to sustain compliance with FISMA and introduce best practices for our information technology and information systems.

This effort has already begun. We recently reached out to agency contacts at the National Credit Union Administration and the Federal Housing Finance Agency, which you graciously provided to us. We have also been in discussions with Department of Homeland Security contacts to review the financial and technical assistance available to small and micro-sized Federal agencies.

In summary, we will move swiftly to improve our Information Assurance Program. I invite the Office of the Inspector General to participate on a regular basis in Information Assurance Program planning and implementation reviews and to offer feedback as the improvement program unfolds.

If you have any questions regarding these comments in response to the Office of Inspector General's draft FISMA evaluation report, please contact Jeff Page, Chief Operating Officer, at 202-606-6632 or Tom Hanley, Acting Chief Information Officer, at 202-606-6618.

Sincerely,

Wendy Spencer
Chief Executive Officer

cc:

Deborah Jeffrey, Inspector General
Asim Mishra, Chief of Staff
Jeffrey Page, Chief Operating Officer
Kim Mansaray, Chief of Program Operations Valerie
Green, General Counsel

Tyler Harding, Principal
Kearney and Company, P.C.
1701 Duke Street, Suite 500
Alexandria, VA 22314

November 4, 2014

Dear Mr. Harding:

As noted in Chief Executive Officer Wendy Spencer's letter of October 22, 2014, the Corporation for National and Community Service concurs with all of the conditions and recommendations in the draft report of Kearney and Company's Fiscal Year 2014 Federal Information Security Management Act (FISMA) Evaluation (Evaluation).

As recommended in your letter we have already formed a nucleus of a FISMA Remediation Team (Team). The initial goal of the Team is to develop a corrective action plan to improve the overall security posture of the agency. To reach this goal the Team will follow the four broad suggestions made in the evaluation. The Team will take a proactive approach to entity-wide risk management with early adoption of the newly issued "Standards of Internal Control in the Federal Government,"[1] leveraging the National Institute of Standards and Technology (NIST) remediation methods, and obtain subject matter expertise to assist in implementing the recommended corrective actions. The Team is actively creating a project management plan to provide oversight of a Plan of Action and Milestones (POA&M) that will address implementing the recommended corrections related to the findings and conditions as described in the Evaluation. It will take several weeks to fully develop a realistic high-level draft of the project management plan.

In the long term the Team will re-develop the agency's entity-wide Information Security Program, which will include performance metrics, as well as outline the security reporting to the Executive Review Board (ERB) . The program will include a POA&M Guide, based on FISMA, NIST, Office of Management and Budget, and Government Accountability Office guidance. The POA&M Guide will serve as a dynamic management tool that will inform the critical steps for addressing programmatic and system-specific vulnerabilities. The Guide will also assist with essential decision-making activities, helping to ensure appropriate oversight and mitigation of security weaknesses and the cost-effective use of resources in resolving weaknesses.

In the short term, a project management plan will be developed to formally document a roadmap for how the Team will implement corrective actions. The plan wilt define how the process will be managed, executed, and controlled. The plan will not be static. It will be a living document and will be continually refined, revised, and updated as appropriate. The Plan will consist of 5 major management processes

[1] Standards for Internal Control in the Federal Government, by the Comptroller General of the United States, United States Accountability Office, GA0-14-704-G, September 2014, effective October 1,2015.

(initiating, planning, executing, monitoring, and closing) and nine management components (integration, scope, time, cost, quality, human resource, communication, risk, and procurement). The high level draft plan is attached as Exhibit 1. The project elements will be tracked through the POA&M processes and at a minimum address the FISMA weaknesses and delineate the tasks necessary to mitigate them as presented in the Evaluation. This approach is presented in Exhibit II.

If you have any questions regarding this letter please contact Tom Hanley, Acting Chief Information Officer, at 202-606-6618.

cc:
Deborah Jeffrey, Inspector General
Asim Mishra, Chief of Staff
Kimberly Mansaray, Chief of Program Operations
Valerie Green, General Counsel

Processes	Initiating	Planning	Executing	Monitoring	Closing
Integration	Project Charter - 11/12/14	Project Management Plan	Direct and Manage Project Execution	• Monitor and Control Project Work • Integrated Change Control	Close Project
Scope		• Defined - 11/14/14 • Create WBS		• Verification • Control	
Time		Activity- • Definition ; • Sequencing; • Resource estimating; • Duration estimating; • Schedule development.		Schedule Control	
Cost		• Estimating • Budgeting		Control	
Quality		Planning	Assurance	Control	Sign off
Human Resource		Skills - Roles and Responsibilities	• Acquire • Develop	Manage	
Communications		Planning	Distribution	• Performance reporting • Manage Stakeholders	
Risk		• Identification Priority • Analysis quantitative and qualitative • Mitigation	Mitigation	Sustaining	
Procurement		Hire, in-house, outsource, contract	Vehicle	Contract administration	Close Out

Exhibit II POA&M Plan and Processes (consist of):

- Conducting periodic reporting on corrective action plans {CAPS) to the Internal Control Governance Body;
- Consistently using a standard CAP reporting worksheet for reporting:
- Presenting the progress of the project plan as a whole to the ERB;
- Planning and monitoring corrective actions;
- Defining roles and responsibilities by using the six sigma RACIS approach. This consists of determining who is Responsible, who is Accountable, who needs to be Consulted, who needs to be Informed, and who needs to provide Support;
- Assisting in identifying the security funding requirements necessary to mitigate weaknesses;
- Scheduling dates of completion will be determined based on a realistic estimate of the amount of time it will take to allocate the required resources, implement the corrective action(s), and complete all associated milestones
- Tracking and prioritizing resources;
- Determining the requirements for closing a finding; and
- Establishing a verification process for completion.

The CAP Management Worksheet – will be a matrix of each finding and will consist of the following attributes:

- Tracking Number - a tracking number that is assigned to the weakness.
- Recommendation Number – This is the number assigned to the individual recommendations or corrective action.
- Risk Identified {FISMA Metric Area) - the source of where the finding/action item was found and the associated finding numbers are entered in this column.
- Weakness -the description of the detailed finding/action item identified in the report.
- Risk Level - the risk level assigned to the finding by the annual report. In the future it would be high medium or low by a reviewer.
- POC - identity the name of the Point of Contact {POC), position/ title and organizational entity that the component head will hold responsible for resolving the finding/action item.
- Resources Required (Cost} -estimated staff time in hours required to resolve the finding/action
  item and identify any cost (e.g. contract costs) associated with resolving the finding/action item.
- Milestones - this is the corrective action.
- Milestones Completion Dates - key milestones with completion dates identifying specific requirements or key steps to correct an identified finding/action item. If the finding/action item has two or more identified issues or elements contributing

to the overall finding/action item,
the milestones and completion dates must be comprehensive enough to address all elements of the finding/action item. They serve as specific, action-oriented steps necessary to mitigate each weakness. The number of milestones articulated per weakness should directly correspond to the number of steps or corrective actions necessary to fully address and resolve the weakness. Milestones should effectively communicate the major steps that will be performed to mitigate a weakness.

- Changes to Milestones - only needs to be completed if the CAP cannot be completed by the Milestones Completion Date or the Scheduled Completion Date cannot be met. This column would include new completion dates for particular milestones or scheduled completion date. The reason for the change must be recorded in "Comments."
- Completion Date -the date that all the milestones have been completed.
- Status – limited to "open", "on-going", "delayed" or "completed." If "delayed", an entry must be made in "Changes to Milestones" with new completion dates for the particular milestone. The reason for the change must be recorded in "Comments."
- Comments - a brief summary of the work accomplished during the reporting period.. An entry is also required if a scheduled completion date or milestones date is missed (record the reason) or if the finding/action item has been corrected and all work is deemed "completed" (record the date of completion). Record any additional details or clarification for any previous entries as well as the application/system name related to the finding in this field.

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

Kearney & Company, P.C. (referred to as "Kearney," "we," and "our") issued 16 Notices of Findings and Recommendations (NFR) to the Corporation for National and Community Service (Corporation) as a result of the fiscal year (FY) 2014 Federal Information Security Management Act of 2002 (FISMA) Independent Evaluation. The 16 NFRs contained information on the condition of the finding and 67 recommendations to mitigate the conditions presented. The Corporation provided a response to the draft FISMA evaluation report. The Corporation "concurs with all of the conditions and recommendations in the draft report." A FISMA Remediation Team was formed to begin prompt creation of corrective action plans and an implementation schedule for those plans. The FISMA Remediation Team will report monthly to the Executive Review Board on their progress to remediate identified security and privacy weaknesses.

Kearney would like to thank the Corporation for the cooperation lent to us during the FISMA evaluation process and the opportunity to assist in improving the security posture of the Corporation.

APPENDIX E: RESPONSES TO DHS'S FY 2014 IG FISMA REPORTING METRICS

FY 2014 IG FISMA Metrics

1: CONTINUOUS MONITORING MANAGEMENT		Answer
1.1. Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		No
1.1.1.	Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7). (AP)	No
1.1.2.	Documented strategy for information security continuous monitoring (ISCM). (AP)	No
1.1.3.	Implemented ISCM for information technology assets. (AP)	No
1.1.4.	Evaluate risk assessments used to develop their ISCM strategy. (AP)	No
1.1.5.	Conduct and report on ISCM results in accordance with their ISCM strategy. (AP)	No
1.1.6.	Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, 800-53A). (AP)	No
1.1.7.	Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A). (AP)	No
1.2 Please provide any additional information on the effectiveness of the organization's Continuous Monitoring Management Program that was <u>not noted</u> in the questions above.		
1.2 Response: The Corporation has not developed, adopted, formally documented, and implemented an organization-wide ISCM strategy and program. Current monitoring practices would be improved by an ISCM strategy that extends to all of the organization's activities, mission/business processes, and information systems tiers. The Corporation for National and Community Service (Corporation) identified the need for the development of a monitoring strategy for each system in its Information Assurance Strategic Plan, dated October 2012.		

2: CONFIGURATION MANAGEMENT		Answer
2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		No
2.1.1.	Documented policies and procedures for configuration management. (Base)	Yes
2.1.2.	Defined standard baseline configurations. (Base)	Yes
2.1.3.	Assessments of compliance with baseline configurations. (Base)	No
2.1.4.	Process for timely (as specified in organization policy or standards) remediation of scan result deviations. (Base)	No
2.1.5.	For Windows-based components, USGCB secure configuration settings are fully implemented, and any deviations from USGCB baseline settings are fully documented. (Base)	No
2.1.6.	Documented proposed or actual changes to hardware and software configurations. (Base)	Yes
2.1.7.	Process for timely and secure installation of software patches. (Base)	No
2.1.8.	Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2). (Base)	No
2.1.9.	Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2). (Base)	No
2.1.10.	Patch management process is fully developed, as specified in organization policy or standards (NIST SP 800-53: CM-3, SI-2). (Base)	Yes
2.2. Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was <u>not noted</u> in the questions above.		
2.2. Response: Multiple opportunities exist to improve the Corporation's security configuration management processes. Specifically, the Corporation does not periodically scan for USGCB compliance and upon the evaluator's request, was not able to produce a report highlighting differences between USGCB settings and deployed configurations. Further, the Corporation did not implement controls to prevent the use of unauthorized portable storage devices on the Corporation's network and clearly communicate whether personal USB storage devices, smart phones, or tablets may be connected the Corporation's desktops. The Corporation conducted monthly vulnerability scans of servers, but Corporation employees and contractors did not review the vulnerability results for 10 consecutive months and the same 39 high risk vulnerabilities repeated each month. They did not scan desktops, laptops or other network devices, nor did they scan all of the servers. Finally, the Corporation did not properly isolate its Voice over Internet Protocol (VoIP) network traffic and prevent desktops on the data network from communicating with VoIP phones and other voice infrastructure.		
2.3	Does the organization have an enterprise deviation handling process and is it integrated with the automated capability. (Base)	Yes
2.3.1.	Is there a process for mitigating the risk introduced by those deviations? (Base)	Yes

3: IDENTITY AND ACCESS MANAGEMENT		Answer
3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?		Yes
3.1.1.	Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1). (Base)	Yes
3.1.2.	Identifies all users, including Federal employees, contractors, and others who access organization systems (NIST SP 800-53, AC-2). (Base)	Yes
3.1.3.	Identifies when special access requirements (e.g., multi-factor authentication) are necessary. (Base)	Yes
3.1.4.	If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2). (KFM)	Yes
3.1.5.	Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11). (AP)	Yes
3.1.6.	Organization has adequately planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).	Yes
3.1.7.	Ensures that the users are granted access based on needs and separation-of-duties principles. (Base)	No
3.1.8.	Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users. (For example: IP phones, faxes, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts.) (Base)	Yes
3.1.9.	Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.) (Base)	Yes
3.1.10.	Ensures that accounts are terminated or deactivated once access is no longer required. (Base)	Yes
3.1.11.	Identifies and controls use of shared accounts. (Base)	Yes
3.2 Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.		
3.2 Response: The Corporation did not complete documentation of where segregation of duties (SoD) must exist for the eSPAN application; therefore, it cannot be ensured that users are granted access based on needs and SoD. This issue has been recurring for the past four years, without meaningful progress, although the Corporation has repeatedly stated that it is working on an assessment to define the required segregation of duties across all business processes and align this with its IT systems. The Corporation states that its status as a government corporation exempts it from Homeland Security Presidential Directive (HSPD) 12 and FIPS 201 requirements to implement Personal Identity Verification (PIV) cards for logical access. The Corporation voluntarily implemented PIV cards for		

3: IDENTITY AND ACCESS MANAGEMENT	Answer
physical access.	

4: INCIDENT RESPONSE AND REPORTING		Answer
4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
4.1.1.	Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1). (Base)	Yes
4.1.2.	Comprehensive analysis, validation, and documentation of incidents. (KFM)	Yes
4.1.3.	When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (KFM)	No
4.1.4.	When applicable, reports to law enforcement within established timeframes (SP 800-61). (KFM)	Yes
4.1.5.	Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (KFM)	Yes
4.1.6.	Is capable of tracking and managing risks in a virtual/cloud environment, if applicable. (Base)	Yes
4.1.7.	Is capable of correlating incidents. (Base)	Yes
4.1.8.	Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, NIST SP 800-61; OMB M-07-16, OMB M-06-19). (Base)	No
4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.		
4.2 Response: The Corporation has not properly classified all computer security incidents nor has it reported all computer security incidents to the United States-Computer Emergency Readiness Team (US-CERT). Additionally, the Corporation relied on an obsolete and unsupported vendor tool for network audit log aggregation and automatic alerting. Due to the tool's age, it has not kept abreast of changes in audit log aggregation and has more limited audit log analysis capabilities than modern tools.		

5: RISK MANAGEMENT		Answer
5.1. Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		No
5.1.1.	Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. (Base)	Yes
5.1.2.	Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1. (Base)	No
5.1.3.	Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800-37, Rev. 1. (Base)	No
5.1.4.	Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev. 1. (Base)	Yes
5.1.5.	Has an up-to-date system inventory. (Base)	Yes
5.1.6.	Categorizes information systems in accordance with government policies. (Base)	Yes
5.1.7.	Selects an appropriately tailored set of baseline security controls. (Base)	Yes
5.1.8.	Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation. (Base)	No
5.1.9.	Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Base)	No
5.1.10.	Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable. (Base)	No
5.1.11.	Ensures information security controls are monitored on an ongoing basis, including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials. (Base)	No
5.1.12.	Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization. (Base)	No
5.1.13.	Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO). (Base)	Yes

5: RISK MANAGEMENT		Answer
5.1.14.	Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks. (Base)	No
5.1.15.	Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies (NIST SP 800-18, NIST SP 800-37). (Base)	Yes
5.1.16.	Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems. (Base)	No
5.2 Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.		
5.2 Response: The Corporation has not developed a Risk Management Program consistent with FISMA requirements, Office of Management and Budget (OMB) policy, and applicable National Institute of Standards and Technology (NIST) guidelines. Specifically, the Corporation has not implemented the NIST Risk Management Framework (RMF), as described in NIST Special Publication (SP) 800-37, Revision (Rev.) 1; and NIST SP 800-39 at the Tier 1: Organizational and Tier 2: Mission/Business levels. Further, the Corporation did not develop corporate standards for its multiple IT contractors to follow regarding ongoing security assessments and continuous monitoring activities. In addition, security assessors did not have sufficient organizational independence to objectively assess and report on security control effectiveness. Resulting outcomes such as SSPs, SARs, and POA&Ms from security assessments contained multiple factual errors and omissions such that a credible, risk-based decision to authorize the system could not occur. Additionally, the Corporation does not exercise sufficient oversight/quality assurance of contractor security measures to identify deficiencies in their information security practice.		

6: SECURITY TRAINING		Answer
6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
6.1.1.	Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1). (Base)	Yes
6.1.2.	Documented policies and procedures for specialized training for users with significant information security responsibilities. (Base)	Yes

6: SECURITY TRAINING		Answer
6.1.3.	Security training content based on the organization and roles, as specified in organization policy or standards. (Base)	No
6.1.4.	Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training. (KFM)	Yes
6.1.5.	Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training. (KFM)	No
6.1.6.	Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, NIST SP 800-53). (Base)	Yes
6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.		
6.2 Response: The Corporation has not implemented a formal role-based Information Security Training program that includes regular training updates. The Corporation's current role-based training material consists of PowerPoint slides focused on promoting awareness of assigned responsibilities rather than training, which NIST defines as building knowledge and skills to facilitate the job performance. The Corporation identified the need for the development of a role-based training program in its Information Assurance Strategic Plan, dated October 2012.		

7: PLAN OF ACTIONS AND MILESTONES (POA&M)		Answer
7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		No
7.1.1.	Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation. (Base)	Yes
7.1.2.	Tracks, prioritizes, and remediates weaknesses. (Base)	No
7.1.3.	Ensures remediation plans are effective for correcting weaknesses. (Base)	Yes
7.1.4.	Establishes and adheres to milestone remediation dates. (Base)	No
7.1.5.	Ensures resources and ownership are provided for correcting weaknesses. (Base)	No
7.1.6.	POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk-based decision to not implement a security control) (OMB M-04-25). (Base)	No

7: PLAN OF ACTIONS AND MILESTONES (POA&M)		Answer
7.1.7.	Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3; OMB M-04-25). (Base)	No
7.1.8.	Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5; OMB M-04-25). (Base)	Yes
7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.		
7.2 Response: The Corporation did not have an adequate POA&M management process in place to ensure all known security weaknesses are recorded, resources identified, and adequately monitored to include timely resolution. 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.		

8: REMOTE ACCESS MANAGEMENT		Answer
8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
8.1.1.	Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17). (Base)	Yes
8.1.2.	Protects against unauthorized connections or subversion of authorized connections. (Base)	Yes
8.1.3.	Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1). (Base)	Yes
8.1.4.	Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1). (Base)	Yes
8.1.5.	If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3). (KFM)	Yes
8.1.6.	Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms. (Base)	Yes
8.1.7.	Defines and implements encryption requirements for information transmitted across public networks. (KFM)	No
8.1.8.	Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required. (Base)	Yes
8.1.9.	Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines). (Base)	Yes

8: REMOTE ACCESS MANAGEMENT		Answer
8.1.10.	Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4). (Base)	Yes
8.1.11.	Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6). (Base)	Yes
8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.		
8.2 Response: The Corporation-issued laptops automatically connect to the Virtual Private Network (VPN) server upon user authentication to the Windows desktop using a shared, rather than a unique, digital certificate that has been issued to all the Corporation's laptops. This configuration does not meet the two-factor authentication requirements for Federal agencies in OMB M-06-16, which states "…allow remote access only with two-factor authentication 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 140-2 encryption and authentication algorithms.		
8.3	Does the organization have a policy to detect and remove unauthorized (rogue) connections?	Yes

9: CONTINGENCY PLANNING		Answer
9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		No
9.1.1.	Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1). (Base)	Yes
9.1.2.	The organization has incorporated the results of its system's Business Impact Analysis (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (NIST SP 800-34). (Base)	No
9.1.3.	Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34). (Base)	No
9.1.4.	Testing of system-specific contingency plans. (Base)	No
9.1.5.	The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34). (Base)	No
9.1.6.	Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	No
9.1.7.	Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans. (Base)	No

9: CONTINGENCY PLANNING		Answer
9.1.8.	After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34). (Base)	No
9.1.9.	Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.10.	Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).	Yes
9.1.11.	Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53). (Base)	Yes
9.1.12.	Contingency planning that considers supply chain threats. (Base)	Yes
9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was <u>not noted</u> in the questions above.		
9.2 Response: The Corporation has an alternate processing site for its data center and annually tests its ability to recover key servers at the alternate site. However, the Corporation's Disaster Recovery documentation does not include plans for all of the Corporation's essential functions and missions. The Business Impact Analysis (BIA) specifically states that it is not meant to address all essential business functions, and the functions were not covered in the Continuity of Operations Plan (COOP) or the Corporation DRP. The Corporation's DRP is written specifically for the general support system and is not representative of the Corporation as a whole, including other key IT contractors and systems. Further, the Corporation has not conducted adequate planning or testing of its COOP. Additionally, the Corporation did not conduct annual testing of its financial system, Momentum.		

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

10: CONTRACTOR SYSTEMS		Answer
10.1.3.	A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud. (Base)	Yes
10.1.4.	The inventory identifies interfaces between these systems and organization-operated systems (NIST SP 800-53: PM-5). (Base)	Yes
10.1.5.	The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates. (Base)	Yes
10.1.6.	The inventory of contractor systems is updated at least annually. (Base)	Yes
10.1.7.	Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines. (Base)	No
10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.		
10.2 Response: Weaknesses with the Corporation's Continuous Monitoring program negatively affected the Corporation's oversight of its IT vendors. For example, the Corporation has not established any performance metrics related to information security for any of its IT contracts. Similarly, weaknesses with the Corporation's Risk Management program affect the Corporation's oversight of contractor systems. Outcomes from risk management activities such as system security plans, SARs, and POA&Ms contained errors and omissions that were not detected and corrected by the Corporation's oversight processes. While the Corporation has developed certain security oversight policies for contractors, it did not assign this oversight responsibility to specific individuals or positions, leaving no one accountable.		

11: SECURITY CAPITAL PLANNING		Answer
11.1. Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?		Yes
11.1.1.	Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process. (Base)	Yes
11.1.2.	Includes information security requirements as part of the capital planning and investment process. (Base)	Yes
11.1.3.	Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2). (Base)	Yes
11.1.4.	Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3). (Base)	Yes
11.1.5.	Ensures that information security resources are available for expenditure as planned. (Base)	Yes

11: SECURITY CAPITAL PLANNING	Answer
11.2 Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.	
11.2 Response: No additional information.	

APPENDIX F: RESULTS FROM FIELD OFFICE ASSESSMENTS

The Corporation for National and Community Service (Corporation) has five National Civilian Community Corps (NCCC) campuses, one Volunteer's in Service to American (VISTA) Member Support Unit campus, and many state offices in cities throughout the United States. In support of the Federal Information Security Management Act of 2002 (FISMA) evaluation of the Corporation, Kearney & Company, P.C. (Kearney) conducted four site visits. Field office assessments were conducted at the Texas State Office, the Iowa State Office, the NCCC North Central Regional, and the Volunteer's in Service to American Member Support Unit (VMSU). As part of Kearney assessment strategy, workspace and office suite areas were inspected for personally identifiable information (PII) exposures. Kearney's visits to these locations also included an evaluation of controls to ensure acceptable usage of Corporation network resources, physical security, rogue connections, PII management, and a search for inappropriate material on Corporation workstations.

At each location, Kearney toured the facilities and noted the physical locations for storage of PII (paper and portable electronic). Kearney noted that all locations stored PII records in locked file cabinets in locked rooms. However, Kearney also noted that PII was being held beyond the retention period.[83] Kearney observed deficiencies in physical access controls at the field offices. These issues were verbally communicated to Corporation management at both the field locations and at Headquarters. Kearney did not detect any wireless access points within proximity of the field offices. Kearney noted that the Managed Data Center Services (MDCS) contractor deployed technology to manage the configuration of the Corporation's laptops and deploy security patches.

Scope Limitation – Field Office Scans

The Kearney FISMA Evaluation Team planned to conduct scans of field office work stations to assess:

1. Compliance with the United States Government Compliance Baseline (USGCB) requirements for the Corporation's desktops
2. Success of the Corporation's security patch management process.

Prior to the site visits, the Corporation verbally indicated that the network security configuration would permit off-site vulnerability and compliance scanning for the MDCS-managed desktops and network devices using authenticated credentials (i.e., user ID and password). However, when scans were formally requested, the Corporation indicated that the off-site scans could only be completed by temporarily weakening the firewall protections on the Corporation's desktops and their managed network. Due to this security concern, vulnerability scans of the field offices

[83] See Appendix A, Notice of Finding and Recommendation 16, *Inadequate Controls over Privacy*, for additional information on the inadequacies associated with PII.

did not occur. Therefore, Kearney could not complete test objectives to evaluate USGCB compliance or the ability to timely deploy and remediate desktop security vulnerabilities.

APPENDIX G: ABBREVIATIONS AND ACRONYMS

Acronym	Definition
AO	Authorizing Official
ARP	Address Resolution Protocol
ATO	Authority to Operate
BPA	Blanket Purchase Agreement
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BYOD	Bring-Your-Own-Device
C&A	Certification and Accreditation
CD	Compact Disk
CEO	Chief Executive Officer
CET	Continuity of Operations Plan Executive Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CIGIE	Council of Inspectors General on Integrity and Efficiency
CNCS	Corporation for National and Community Service
CO	Contracting Officer
COO	Chief Operating Officer
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
Corporation	Corporation for National and Community Service
COTS	Commercial-off-the-Shelf
CPIC	Capital Planning and Investment Control
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DRP	Disaster Recovery Plan
DVD	Digital Video Disk
E-Gov	E-Government Act of 2002
EOL	End-of-Life
ERB	Executive Review Board
eSPAN	Electronic System for Programs Agreements and National Service Participants
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FY	Fiscal Year

Acronym	Definition
GAO	Government Accountability Office
GSS	General Support System
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HQ	Headquarters
IAP	Information Assurance Plan
IATO	Interim Authority to Operate
ID	Identification
IG	Inspector General
IO	Information Owner
IP	Internet Protocol
IPSec	Internet Protocol Security
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Managers
ISSO	Information System Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
Kearney	Kearney & Company, P.C.
LAN	Local Area Network
MA	Major Application
MAC	Media Access Control
MARS	Monitoring Analysis and Reporting System
MDCS	Managed Data Center Services
MPLS	Multi-Protocol Label Switching
MVM	McAfee Vulnerability Manager
NARA	National Archives and Records Administration
NCCC	National Civilian Community Corps
NFR	Notice of Finding and Recommendation
NIST	National Institute for Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
OS	Operating System
PBX	Private Branch Exchange
PCCB	Production Change Control Board

Acronym	Definition
PIA	Privacy Impact Assessments
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
POA&M	Plan of Actions & Milestones
PSTN	Public Switched Telephone Network
PUB	Publication
PWS	Performance Work Statement
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SAR	Security Authorization Report
SCAP	Security Content Automation Protocol
SIP	Session Initiation Protocol
SoD	Segregation of Duties
SOW	Statement of Work
SP	Special Publication
SSL	Secure Socket Layer
SSP	System Security Plan
TBD	To Be Determined
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
TO	Task Order
TRUST	National Service Trust
U.S.C.	United States Code
USB	Universal Serial Bus
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Compliance Baseline
VA	Department of Veterans Affairs
VISTA	Volunteers In Service To America
VLAN	Virtual Local Area Network
VMSU	Volunteer's in Service to American Member Support Unit
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX H: REFERENCED DOCUMENTS

Federal Law:

- Federal Information Security Management Act of 2002 (FISMA) (Title III, Public Law [P.L.] No. 107-347)
- Privacy Act of 1974 (P.L. No. 93-579)
- e-Government Act of 2002 (P.L. No. 107-347).

Office of Management and Budget (OMB):

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

Federal Information Processing Standards (FIPS):

- 199, *Standards for Security Categorization of Federal Information and Information Systems*
- 140-2, *Security Requirements for Cryptographic Modules.*

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

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

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

- 800-16, Inform*ation Technology Security Training Requirements: A Role- and Performance-Based Model*
- 800-18, Revision (Rev.) 1, *Guide for Developing Security Plans for Federal Information Systems*
- 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- 800-39, *Managing Information Security Risk*
- 800-52, Rev. 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
- 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
- 800-55, *Performance Measurement Guide for Information Security*

- 800-58, *Security Considerations for Voice Over IP Systems*
- 800-61, *Revision 2, Computer Security Incident Handling Guide*
- 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
- 800-92, *Guide to Computer Security Log Management*
- 800-111, *Guide to Storage Encryption Technologies*
- 800-113, *Guide to SSL VPNs*
- 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organization.*

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

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

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

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

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