

Office of Inspector General
Corporation for National and
Community Service

**FEDERAL INFORMATION SYSTEM
MANAGEMENT ACT (FISMA) REVIEW FOR FY 2011
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE**



Corporation for
**NATIONAL &
COMMUNITY
SERVICE** 

FINAL

NOVEMBER 10, 2011

Prepared by:

Richard S. Carson & Associates, Inc.
4720 Montgomery Lane, Suite 800
Bethesda, Maryland 20814

TABLE OF CONTENTS

Executive Summary ii
 Results in Brief ii

Abbreviations And Acronymsiv

Referenced Documents..... v

General Overview..... 1

Independent Evaluation 1

Security Program Evaluation..... 2
 CONCLUSIONS 2

Evaluation of Agency Oversight of Contractor 3
 CONCLUSIONS 3

Evaluation of Agency Plan of Action and Milestones (POA&M) Process..... 3
 CONCLUSIONS 3

State Field Office Assessments 4
 CONCLUSIONS 4
 RECOMMENDATIONS 4

Appendix A – Detailed Findings and Recommendation..... 5

Appendix B – Corporation Management Response 7

EXECUTIVE SUMMARY

The Office of Inspector General (OIG), Corporation for National and Community Service (Corporation) contracted with Richard S. Carson & Associates, Inc. (Carson) to perform a Fiscal Year (FY) 2011 independent Federal Information Security Management Act (FISMA) evaluation of the Corporation's information technology systems, controls, and policies. The objectives of the evaluation were to:

- Determine the efficiency and effectiveness of the Corporation's information security policies, procedures, and practices
- Review network/system security of a representative subset of the Corporation's systems
- Assess the Corporation's compliance with FISMA and related information security policies, procedures, standards, and guidelines
- Assess the Corporation's progress in correcting weaknesses identified in prior-year FISMA evaluations
- Evaluate personally identifiable information (PII) protection and physical controls at field office sites

RESULTS IN BRIEF

The Corporation has taken significant steps to enhance its information security program and address issues identified in the FY 2010 FISMA report, including the following:

- The Certification and Accreditation (C&A) process has been re-worked to ensure full compliance with the National Institute of Standards and Technology (NIST) guidance, provide better documentation, and increase assurance that controls have been adequately assessed. Specific improvements include:
 - Continued development of policies and procedures;
 - Continued oversight of the technology contractor SRA International, Inc. (SRA) and other contracted services;
 - Scanning to include field office site networks and Corporation headquarters systems;
 - Continued training in proper protection and handling of PII information for field office staff; and
 - Documentation of processes and controls

We have made five recommendations in areas needing improvement to further enhance compliance with the Corporation's information security program. The recommendations are summarized on page 5 of this report.

Corporation Response

Carson will review the Corporation's response to the Notification of Findings and Recommendations, which will be included as Attachment B.

BACKGROUND

On December 17, 2002, President George W. Bush signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002.

FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal Government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

FISMA requires all Federal agencies to implement and maintain information security policies, procedures, and control techniques to ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access, or modification of such information.

ABBREVIATIONS AND ACRONYMS

C&A	Certification and Accreditation
CCB	Change Configuration Board
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Plan
E-SPAN	Electronic-System for Programs, Agreements, and National Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSS	General Support System
IG	Inspector General
ISSO	Information System Security Officer
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SDLC	System Development Life Cycle
SETA	Security Education, Training, and Awareness
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team

REFERENCED DOCUMENTS

Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347)

Office of Management and Budget (OMB)

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

NIST Federal Information Processing Standards (FIPS)

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

NIST Special Publications (SP)

800-18, Revision 1, *Guide for Developing Security Plans for Information Technology Systems*
800-30, *Risk Management Guide for Information Technology Systems*
800-34, Revision 1, *Contingency Planning Guide for Information Technology Systems*
800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*
800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems*
800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
800-83, *Guide to Malware Incident Prevention and Handling*
800-100, *Information Security Handbook: A Guide for Managers*

GENERAL OVERVIEW

FISMA section 3542(b)(1)(A),(B),(C) defines information security as "... protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity—guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; (B) confidentiality—preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability—ensuring timely and reliable access to and use of information."

INDEPENDENT EVALUATION

Field work for this independent evaluation was conducted from June through October 2011 and covered the following Corporation systems: the Corporation network (Network GSS); Electronic System for Programs, Agreements and National Service (E-SPAN), and the HP-Helpdesk. Our evaluation methodology is compliant with the Council of Inspectors General on Integrity and Efficiency (CIGIE), "Quality Standards for Inspections and Evaluations," and consists of inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls in order to conclude the evaluation.

This section provides the conclusions of our research, analysis, and assessment of the Corporation's information security program, policies, and practices. Compliance with security policy, standards, and guidance prescribed by the Office of Management and Budget (OMB), the National Institute for Standards and Technology (NIST), and related authoritative policies, procedures, standards, and guidelines (criteria), where applicable, are cited when describing a specific condition.

The Corporation has taken significant steps to enhance its information security program and address issues identified in prior FISMA evaluations. It has outsourced its technology activities with regard to Network core services, as well as the Exchange services, Blackberry Enterprise services, and "shared" drive services to SRA International, Inc. The Corporation and SRA are in the process of addressing procedures in the following areas:

- System security plan
- POA&M execution and continuous monitoring
- Policy and procedures

SECURITY PROGRAM EVALUATION

FISMA requires 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 by or managed by another agency, contractor, or other sources. NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers*, identifies information security program elements that are expected to be incorporated into information security programs across the Federal sector.

CONCLUSIONS

The Corporation has documented an Information Security Program Plan that adequately addresses security program elements recommended by NIST guidance, including:

- Formal information security governance structure
- Integrating security into the System Development Life Cycle (SDLC)
 - Periodic assessments of risk
 - Policies and procedures that are based on these risk assessments
- Security awareness training
- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls
 - A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization
 - Configuration management processes to manage the effects of changes or differences in configurations on an information system or network
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization

EVALUATION OF AGENCY OVERSIGHT OF CONTRACTOR

FISMA requires that Federal agencies perform oversight and evaluations to ensure information systems used or operated by a contractor, or other organization on behalf of the agency, meet the requirements of FISMA, OMB policy, NIST guidelines, and Corporation policy. FISMA Section 3544(a) (1) (A) (ii) describes Federal agency security responsibilities as including “information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.” Section 3544(b) requires that each agency provide information security for the information and “information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”

OMB Memorandum 07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* states: “Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency. Agencies and service providers have a shared responsibility for FISMA compliance.”

The Corporation in FY 2009 began an effort to outsource the hosting and maintenance of information assets associated with its Network core services, Exchange services, Blackberry Enterprise services, and “Shared” drive services. It completed the outsourcing and equipment migration effort in early FY 2010 to SRA International, Inc.

CONCLUSIONS

The Corporation maintains oversight of SRA through weekly meetings with SRA’s Information System Security Officer (ISSO) in which all tasks conducted are reviewed and planned. The Corporation’s Chief Information Security Officer (CISO) and SRA’s ISSO meet weekly for service updates and also use the Change Control Board (CCB) to monitor the progress of the vendor. A Weekly Transition and Operations meeting is conducted with the COTR, the ISSO, Corporation personnel, and other SRA personnel. The Corporation has documented contract requirements that include continuous monitoring language.

EVALUATION OF AGENCY PLAN OF ACTION AND MILESTONES (POA&M) PROCESS

OMB guidance on FISMA implementation requires agencies to identify and report on significant deficiencies in their information security program. A significant deficiency is a weakness in the agency’s overall information system security program or management control structure, or within one or more information systems, that significantly restricts the capability of agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

CONCLUSIONS

The Corporation’s Information Security Policy requires that POA&Ms be maintained for the security program and for each major system. It also requires that any official reports providing specific information on weaknesses or vulnerabilities resulting from OIG audits, reviews, or scanning activity related to such work as risk assessments, certification testing, or penetration testing be documented and tracked as part of the specific system POA&M documentation.

POA&Ms for the E-Span and the network systems have been documented and are being addressed. Most of the POA&M milestone and completion dates are based on the completion of the outsourcing and data center migration in FY 2010. No exceptions were found with the POA&M tracking and vulnerability mitigation process. This was verified by review of the POA&M documentation from the FY 2010 C&A process.

STATE FIELD OFFICE ASSESSMENTS

State field office assessments were conducted on three state field offices and one AmeriCorps National Civilian Community Corps (NCCC) campus, evaluating environmental controls, physical controls, and PII protection. The following sites were reviewed: Detroit, MI; Minneapolis, MN; Sacramento, CA; and Los Angeles, CA. As part of our assessment strategy, workspace and office suite areas were inspected for PII exposure.

CONCLUSIONS

The field office findings included instances of PII information exposure, PII hardcopy violations, drive storage violations, physical access violations, and infrastructure physical protection issues.

RECOMMENDATION

We recommend that the existing Corporation policy for protecting and handling of PII be referenced and enforced. All forms of PII (paper and electronic) must be stored in designated file cabinets. Recycling bins used to store PII before it can be properly destroyed must be secured to prevent unauthorized access.

APPENDIX A – DETAILED FINDINGS AND RECOMMENDATION

Findings and Recommendations

Notification of Finding # 1: The ESPAN annual assessment test plan and test documentation is insufficient because it does not provide procedures for testing controls, the dates when the controls are tested, or links to the source documentation to show evidence of the testing.

Recommendation(s)

We recommend that CNCS conduct annual assessments in a more structured, planned process that provides detailed information regarding test dates, explanation of testing procedures, and links from the controls to the source documents.

Notification of Finding # 2: There are no agreements defining the level of service for the HP help desk's fax location or documentation stating that the fax location is in compliance with CNCS security requirements. The Certification and Accreditation documentation lists four areas within the HP boundary: Chicago, IL; Santa Clara, CA; London, KY; and Orlando, FL. The Montgomery, AL, facility is not included within the C&A boundary.

Recommendation(s)

We recommend that CNCS require HP to develop an SLA or provide C&A documentation for the fax location in Montgomery. We also recommend that the Montgomery facility be included within the C&A boundary to ensure that the proper security controls are in place to protect CNCS information.

Notification of Finding # 3: There is no Service Level Agreement (SLA) or Certification and Accreditation documentation for the SRA help desk regarding its use of a third-party vendor, ServiceNow (HP help desk's Fax location), to document and track help desk calls and requests for the CNCS network and computing environment.

Recommendation(s)

We recommend that SRA include the ServiceNow server as part of the CNCS network boundary and require SRA to provide either a SLA or C&A documentation for it.

Notification of Finding # 4: Personally Identifiable Information (PII) was found exposed in the office suite of the Michigan State office. Documents were found containing names, Social Security Numbers (SSN), and addresses in a box in an open, unlocked supply room.

Recommendation(s)

We recommend that CNCS require all office directors to conduct semiannual office walk-throughs to detect instances of unsecured PII. If a violation is detected, PII documents should be secured or disposed of in a secure manner. The results of the walk-through should be reported to the Chief Information Security Officer or designee.

Notification of Finding # 5: Our review of the CNCS Information Security Policies (CNCS ISP) disclosed several references to a CNCS record retention policy. However, we were not provided a copy of this policy and, therefore, could not validate its' existence.

Recommendation(s)

We recommend that CNCS develop a record retention policy that speaks directly to the procedures required by NARA and issue this policy to field office directors.

APPENDIX B – CORPORATION MANAGEMENT RESPONSE

November 9, 2011

TO: Robert J. Walters
Assistant Inspector General Investigations

THRU: Robert Velasco, II
Acting Chief Executive Officer

FROM: Philip Clark
Chief Information Officer

Subject: Corporation Comments on OIG FISMA Review Report for Fiscal Year 2011

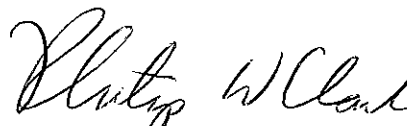
Thank you for the opportunity to comment on the OIG FISMA report for Fiscal Year 2011. As noted in the report, the Corporation has taken steps in FY 2011 to continue to improve its information security program and compliance with FISMA. We acknowledge that there is still work to do, and have a number of initiatives planned for FY 2011 to further enhance the program.

Corporation Response

The Corporation has reviewed and concurred with three of the findings and recommendations presented and did not concur with two of the findings in the report. Indeed, the recommendations are in alignment with CNCS' Strategic Technology and ongoing information assurance projects. Key accomplishments in FY 2011 include:

- Continued updating of information assurance documentation to ensure compliance with NIST and OMB privacy and system security guidance.
- Completed vulnerability scanning of public-facing elements of CNCS systems.
- Hired a system security engineer and acquired scanning software to ensure that new vulnerabilities are not introduced into CNCS systems.
- Continuation of efforts to work with external system providers to the Corporation to comply with FISMA requirements.

The Corporation will continue to review and refine our information security and privacy programs in the upcoming fiscal year. If you have any questions about this response or the planned activities, please contact the Corporation's Chief Information Security Officer, Laurie Young at (202) 606-6662.



Philip W. Clark
Chief Information Officer

**FY 2011 FISMA Independent Evaluation
Corporation for National and Community Services (CNCS)
Finding 1**

Finding # 1: The ESPAN annual assessment test plan and test documentation is insufficient because it does not provide procedures for testing controls, the dates when the controls are tested, or links to the source documentation to show evidence of the testing.

Recommendation(s)

We recommend that CNCS conduct annual assessments in a more structured, planned process that provides detailed information regarding test dates, explanation of testing procedures, and links from the controls to the source documents.

Management Response

- Management concurs with the Notification of Finding.
- Management does not concur with the Notification of Finding.

The Security and Testing Evaluation (ST&E) spreadsheet used by the Corporation has been found acceptable in previous years by Financial Auditors and the FISMA Reviewers. The Corporation's testing control procedures (Assessment Method, Assessment Objects, and Assessment Tool columns fields from the CNCS ST&E spreadsheet) are from the comprehensive set of assessment procedures as described in Appendix F of NIST SP800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*. There has been no recent change to NIST guidance in this area. CNCS sees no need to depart from what has been accepted practice.

The "Projected Review Date" on the spreadsheet reflects either the date that controls were tested (meeting the NIST requirement), or a future date when testing is expected. CNCS will change the title of this column to "Review Date" to eliminate any confusion in the future.

All documentation supporting the test of each control is contained in a separate file folder for each control, meeting the NIST requirement to provide documentation for each control tested. Links in the spreadsheet to the source documentation (Artifacts) is not a requirement by the NIST and is not a valid basis for a finding. However, to make this review easier for auditors, future assessments will link the artifacts to the corresponding control test on the spreadsheet.

OIG Comments

OIG concurs with OIT's statement regarding making changes to the Security and Testing Evaluation spreadsheet to avoid future confusion.

**FY 2011 FISMA Independent Evaluation
Corporation for National and Community Services (CNCS)
Finding 2**

Finding # 2 There are no agreements defining the level of service for the HP help desk's fax location or documentation stating that the fax location is in compliance with CNCS security requirements. The Certification and Accreditation documentation lists four areas within the HP boundary: Chicago, IL; Santa Clara, CA; London, KY; and Orlando, FL. The Montgomery, AL, facility is not included within the C&A boundary.

Recommendation(s)

We recommend that CNCS require HP to develop a SLA or provide C&A documentation for the fax location in Montgomery. We also recommend that the Montgomery facility be included within the C&A boundary to ensure that the proper security controls are in place to protect CNCS information.

Management Response

- Management concurs with the Notification of Finding.
- Management does not concur with the Notification of Finding.

The Corporation agrees that National Service Hotline fax server that resides in London, KY was not assessed during the certification. Various documents are faxed to the National Service Hotline fax server that resides in London, KY. HP Help Desk employees receive, review, and upload via VPN these faxes to a secure share on a CNCS server on behalf of the Trust.

Rather than certify the London, KY fax server, the Corporation will remove the fax server in London, KY and establish a fax server at the CNCS headquarters. HP Help Desk employees will continue to review the faxes, but through a VPN connection between HP and CNCS. The new fax server and its associated controls will be assessed by the CNCS IA staff to ensure compliance with Federal and agency security requirements. The HP Help Desk SSP will also be updated to reflect this change.

The fax location at Montgomery, AL has not stored and will not store data, either as a production or backup facility, and is therefore not subject to certification.

OIG Comments

OIG concurs.

**FY 2011 FISMA Independent Evaluation
Corporation for National & Community Services (CNCS)
Finding # 3**

Finding # 3: There is no Service Level Agreement (SLA) or Certification and Accreditation documentation for the SRA help desk regarding its use of a third-party vendor, ServiceNow, to document and track help desk calls and requests for the CNCS network and computing environment.

Recommendation(s)

We recommend that SRA include the ServiceNow server as part of the CNCS network boundary and require SRA to provide either a SLA or C&A documentation for it.

Management Response

- Management concurs with the Notification of Finding.
- Management does not concur with the Notification of Finding.

CNCS nonconcur with the recommendation to place the ServiceNow application within the CNCS network boundary. ServiceNow does not meet the criteria contained in guidance from the National Institute of Standards and Technology (NIST) SP800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, for determining what elements belong within the network boundary.

The guidance provides that: “The set of information resources allocated to an information system defines the boundary for that system. Organizations have significant flexibility in determining what constitutes an information system and its associated boundary. If a set of information resources is identified as an information system, the resources are generally under the same direct management control... In addition to consideration of direct management control, it may also be helpful for organizations to determine if the information resources being identified as an information system:

- Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements; and
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).”

Therefore, CNCS has designated ServiceNow as an external information system service. As such, ServiceNow should have a SLA or a C&A. NIST also uses ServiceNow and is currently conducting a C&A of that application. CNCS has decided to accept the NIST C&A for CNCS purposes. CNCS has accepted the risk of operating ServiceNow pending the NIST C&A completion (Waiver FY11-013), as has NIST. To mitigate the risk of operating this application while certification is underway the CNCS Information Assurance team is coordinating access to perform monthly non-intrusive vulnerability scans against the ServiceNow servers.

**FY 2011 FISMA Independent Evaluation
Corporation for National & Community Services (CNCS)
Finding # 3**

OIG Comments

OIG concurs with OIT statements regarding the follow: 1) acceptance of NIST C&A for CNCS purposes; and 2) stated plan of action to mitigate the risk of operating the ServiceNow application while certification is underway. OIG also concurs with OIT's statement regarding why ServiceNow should not be part of the CNCS boundary.

**FY 2011 FISMA Independent Evaluation
Corporation for National and Community Services (CNCS)
Finding # 4**

Finding # 4: Personally Identifiable Information (PII) was found exposed in the office suite of the Michigan State office. Documents were found containing names, Social Security Numbers (SSN), and addresses in a box in an open, unlocked supply room.

Recommendation(s)

We recommend that CNCS require all office directors to conduct semiannual office walk-throughs to detect instances of unsecured PII. If a violation is detected, PII documents should be secured or disposed of in a secure manner. The results of the walk-through shall be reported to the Chief Information Security Officer or designee.

Management Response

- Management concurs with the Notification of Finding.
- Management does not concur with the Notification of Finding.

We concur with the finding and will have all office directors conduct semiannual office walkthroughs which will be reported to the CISO. The Michigan office has rectified the situation. They have inventoried the room and ensured that it now contains only materials that are public and promotional in nature, and securely destroyed the document in question and the Michigan State Director review the PII security of the office space and report his findings to his direct supervisor—the North Central Cluster Area Manager—once per quarter.

OIG Comments

OIG concurs.

**FY 2011 FISMA Independent Evaluation
Corporation for National & Community Services (CNCS)
Finding 5**

Finding # 5: Our review of the CNCS Information Security Policies (CNCS ISP) disclosed several references to a CNCS record retention policy. However, we were not provided a copy of this policy and, therefore, could not validate its' existence.

Recommendation(s)

We recommend that CNCS develop a record retention policy that speaks directly to the procedures required by NARA and issue this policy to field office directors.

Management Response

- Management concurs with the Notification of Finding.
- Management does not concur with the Notification of Finding.

The Corporation agrees with this finding and a record retention policy will be developed and issued to the field office directors.

OIG Comments

OIG concurs.