Office of Inspector General
Corporation for National and Community Service

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) REVIEW FOR FY 2010 CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT NUMBER 11-03

FINAL

NOVEMBER 10, 2010

Prepared by:

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

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 an independent Fiscal Year (FY) 2010 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 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 2009 FISMA report, including the following:

- The certification and accreditation (C&A) process has been overhauled 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 in this area include:

    - Continued development and review of policies and procedures
    - Continued oversight of the technology contractor, SRA International Inc. (SRA), and other contracted services
    - Scanning to include site field office networks
    - Continued training in proper protection and handling of PII information for field office personnel
    - Continued efforts to make the entity First Financial Associates become FISMA compliant in order for it to continue conducting Corporation business

We have made three recommendations in areas needing improvement to further enhance compliance through the Corporation's information security program. The recommendations are summarized on page 10 of this report. The findings for First Financial Associates have already been submitted and addressed by the Corporation.

CORPORATION RESPONSE

Carson and the OIG will review the Corporation's response to the draft report, which is (to 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's inspector 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
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
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, *Contingency Planning Guide for Information Technology Systems*
800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
800-53, *Recommended Security Controls for Federal Information Systems*
800-53A *Guide for Assessing the Security Controls in Federal Information Systems*
800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
800-83, *Guide to Malware Incident Prevention and Handling*
800-100, *Information Security Handbook: A Guide for Managers*

TABLE OF CONTENTS

Executive Summary i
Results in Brief i
Corporation Response i
Abbreviations And Acronyms iii
Referenced Documents iv
General Overview 1
Independent Evaluation 1
Security Program Evaluation 2
CONCLUSIONS AND RECOMMENDATIONS 2
Information Security Governance 2
CONCLUSIONS AND RECOMMENDATIONS 3
RECOMMENDATION: 3
Security Awareness and Training 3
CONCLUSIONS 3
Security and the System Development Life Cycle (SDLC) 3
CONCLUSIONS 3
Security Plans 4
CONCLUSIONS 4
Contingency and Continuity of Operations Plans 4
CONCLUSIONS 4
Configuration Management 5
CONCLUSIONS 5
Privacy Impact Assessments 5
CONCLUSIONS 5
Certification and Accreditation (C&A), Security Controls Testing, and Contingency Plan Testing 5
CONCLUSIONS 6
Incident-Handling and Reporting 6
CONCLUSIONS 6
Evaluation of Agency Oversight of Contractor 7
CONCLUSIONS 7
Evaluation of Agency Plan of Action and Milestones (POA&M) Process 7
CONCLUSIONS 7

State Field Office Assessments 8
CONCLUSIONS 8
RECOMMENDATIONS 8
Field office and Headquarters scan 9
CONCLUSIONS 9
RECOMMENDATIONS 9
Appendix A – Detailed Findings and Recommendation 10
Appendix B – Corporation Response 13
Appendix C – Independent Evaluation Federal Information Security Management (FISMA) Compliance of First Financial Associates 14

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

This independent evaluation was conducted from June through October 2010 and covered the following Corporation systems: Corporation Network; Electronic System for Programs, Agreements and National Service (E-SPAN); and AmeriCorps Portal. Our evaluation methodology is compliant with the Council of Inspectors General on Integrity and Efficiency (CIGIE), "Quality Standards for Inspections," and consists of inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls.

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. The Corporation has outsourced its technology activities with regard to network core services, as well as its exchange services, Blackberry Enterprise services and "shared" drive services to SRA, a private contractor This outsourcing of information system maintenance activities is intended to enhance the Corporation's efforts to move toward FISMA compliance and to fully document its procedures, as well as those of SRA. The Corporation and SRA are in the process of addressing procedures in the following areas:

- System inventory
- System security plan
- Continuity of Operations Plan (COOP) and contingency planning
- 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 government.

CONCLUSIONS AND RECOMMENDATIONS

The Corporation has documented an Information Security Program Plan that adequately addresses 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 Corporation's operations and assets

INFORMATION SECURITY GOVERNANCE

Agencies should integrate their information security governance activities with the overall agency structure and activities by ensuring appropriate participation of agency officials in overseeing implementation of information security controls throughout the agency. FISMA requires that the Corporation develop risk-based policies and procedures that cost-effectively reduce risks to an acceptable level and perform an annual assessment of their security program.

CONCLUSIONS AND RECOMMENDATIONS

Key activities that facilitate such integration are strategic planning, establishment of roles and responsibilities, integration with the enterprise architecture, and documentation of security objectives in policies and guidance.

The Corporation has documented its Strategic Plan, the key roles within its IT organizational structure, and has documented information security policies that establish the security requirements for protecting information resources. Standards, guidelines, and procedures have also been developed to provide guidance on implementing these policies. The Corporation has draft policies of its current security posture for the new data center environment and the outsourced technology.

RECOMMENDATION:

We recommend that the Corporation complete policy updates, including the procedures and responsibilities of the Corporation and SRA. The Corporation's policies should correlate with SRA's procedures to show execution and enforcement of the policies.

SECURITY AWARENESS AND TRAINING

FISMA requires security awareness training to inform personnel, including contractors and other information systems users, of the risks associated with their use of Corporation's information assets. Users must also be informed of their responsibilities to comply with agency policies and procedures designed to reduce those risks.

CONCLUSIONS

A formal security awareness training program is in place that is in accordance with the guidance specified in NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*

The Office of Information Technology (OIT) has conducted information technology security awareness training for all users and users with significant information technology security responsibilities, including contractors. Security awareness training is reviewed and implemented annually. Training is conducted through onsite presentations and online awareness courses.

SECURITY AND THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

A number of Federal laws and directives require integrating security into the SDLC, including FISMA and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*. Information security must be integrated into the SDLC to ensure appropriate protection for the information that the system is intended to transmit, process, and store.

CONCLUSIONS

Generally, it was noted that the Corporation has documented policy and procedures that incorporate security into the SDLC. For example, Corporation policy requires that vulnerability assessments be conducted as part of a risk management program. Risk assessment

documentation and the methodology used are compliant with requirements defined by NIST SP 800-30, *Risk Assessment Guide for Information Technology Systems.*

During this period of review, the Corporation completed its transition to a managed data center. The following activities were completed during the certification and accreditation (C&A) assessment conducted in April 2010:

- The completion of the Corporation system inventory that includes an assessment and security categorization of information for all of the Corporation's systems
- Revision of the network Risk Assessment
- Revision of the network Security Plan
- Documentation and testing of network security controls
- Collection of system-related artifacts, such as operation manuals and system administration manuals and guides, contingency plans, and configuration management plans, where applicable.

SECURITY PLANS

The completion of system security plans is a requirement of OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, and Title III of the E- Government Act, the FISMA. The system security plan provides a summary of the security requirements for the information system(s) that support the operations and assets of the agency and describes the security controls in place or planned for meeting those requirements. NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Information Technology Systems,* requires that all information systems be covered by a system security plan and be labeled as a major application or general support system.

CONCLUSIONS

The Corporation has documented system security plans for its GSS and major applications that are substantially compliant with guidance specified in NIST SP 800-18. The current GSS System Security Plan is maintained and updated by the vendor SRA.

CONTINGENCY AND CONTINUITY OF OPERATIONS PLANS

FISMA requires plans and procedures to be in place to ensure continuity of operations in the event of a loss of service. OMB requires contingency planning to be accomplished and periodically tested to ensure an agency or department can continue to provide the necessary IT services and support to continue its assigned mission.

CONCLUSIONS

The Corporation has documented its policy for contingency planning. Disaster recovery testing was conducted from Monday, August 23, 2010, through Friday, August 27, 2010. All testing was fully successful and met recovery requirements.

As previously stated, the Corporation has outsourced much of its information systems infrastructure to external vendors. The primary location for the Corporation's outsourced information assets is the contractor-managed data center, DC3, belonging to SAVVIS in

Sterling, VA. The recovery site for these resources and their capabilities is the SAVVIS data center, OC2, located in Irvine, CA. SRA is responsible for maintaining the Corporation's resources in these facilities, as well as providing staffing for the Network Operations Center (NOC), and the OIT help desk call center from its offices in Fairfax, VA.

CONFIGURATION MANAGEMENT

FISMA requires agencies to have "policy and procedures to ensure compliance with minimally acceptable system configuration requirements."

CONCLUSIONS

The Corporation has issued its security configuration policy through a configuration management plan, configuration management procedures, SDLC methodology, security configuration baselines, change control policy, and patch management and system maintenance policy. The Corporation policy requires the establishment and maintenance of baseline configurations. Baseline configuration standards have been established for the Corporation network, servers, and workstations, and a process is in place to maintain baseline documentation.

PRIVACY IMPACT ASSESSMENTS

FISMA defines information security as a means of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to protect personal privacy and proprietary information.

CONCLUSIONS

The Corporation has policy and procedures in place to ensure that it properly collects and protects personal information about individuals and provides guidance to Corporation staff about information privacy. The Corporation's security policies also call for initiating the privacy impact assessment (PIA) in the early stages of a system's development to ensure that it is completed as part of the required SDLC reviews.

A PIA was conducted and documented in the C&A assessment conducted in April 2010 for all systems reviewed.

CERTIFICATION AND ACCREDITATION (C&A), SECURITY CONTROLS TESTING, AND CONTINGENCY PLAN TESTING

FISMA requires that the "*agency wide information security program*" shall include periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls, to be performed with a frequency depending on risk, but no less than annually. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* requires the following documentation to be included in the security accreditation package:

- Approved System Security Plan
- Security Assessment Report
- Plan of Action and Milestones (POA&M)

CONCLUSIONS

The Corporation conducted a C&A assessment in April 2010. It was conducted during the transition to the SAVVIS data center, which increased the scope of the C&A to include systems housed at the Corporation and SAVVIS. POA&M items were created during the migration and most POA&M items were delayed and dated for completion after the data center move was completed to prevent duplication of effort in the mitigation efforts.

INCIDENT-HANDLING AND REPORTING

FISMA requires agencies to have "procedures for detecting, reporting, and responding to security incidents."

CONCLUSIONS

The Corporation has documented information security policies and procedures that require all Corporation information users to report any suspected information security incidents in accordance with Incident Response Procedures.

The Corporation has procedures in place for incident-handling and reporting. During the review process, the Corporation experienced a breach of its AmeriCorps Portal, which maintains data that varies in sensitivity. In most cases the breach impacted data such as user names, addresses, phone numbers, dates of birth and partial Social Security Numbers. The vulnerabilities that may have allowed the breach to occur affected both AmeriCorps applicants and members. Because of this breach, more than 500,000 notification letters have been sent to individuals who have AmeriCorps Portal accounts. The following steps were executed, as stated in the incident and handling policy and procedures:

Incident:

- Detection
- Notification to U.S. Computer Emergency Readiness Team (US-CERT)

Handling:

- Investigation
- Logging
- Review
- Plan of Action Resolution
- Authority Notification
- Plan of Action and Correction

The remediation process is ongoing with the Corporation, SRA, parties involved with the original development of the Portal, as well as other parties that have been contracted, to conduct internal/external vulnerability tests and a complete source code review of the Portal.

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,* provides the following guidance on page 24: "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 began an effort to outsource the hosting and maintenance of information assets associated with the its network core services, exchange services, Blackberry Enterprise services and "shared" drive services in 2009. It completed the outsourcing and equipment migration effort in early 2010. SRA and SAVVIS were the vendors selected to provide the maintenance and hosting support, respectively, for the outsourcing project.

CONCLUSIONS

The Corporation maintains oversight of the vendor, SRA, through weekly meetings with the ISSO, during which all tasks conducted are reviewed and planned. The Corporation's 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 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 the 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 data center migration, a result of the recent outsourcing activities that were completed in 2010. No exceptions were found with the progress of POA&M tracking and vulnerability mitigation.

STATE FIELD OFFICE ASSESSMENTS

State field office assessments were conducted on 10 offices, evaluating environmental controls, physical controls, and PII protection. The following offices were reviewed: Phoenix, AZ; Chicago, IL; Austin, TX; Concord, NH; Columbia, SC; Albany, NY; Hartford, CT; Richmond, VA; Orlando, FL; and Atlanta, GA. As part of our assessment strategy, workspace and office suite areas were inspected for PII exposure. Also included in the field visits were the VISTA Management Support Unit in Austin, TX, and First Financial Associates in Atlanta, GA, which handles child care subsidy payments for the Corporation.

CONCLUSIONS

The field office findings included PII exposure, PII hardcopy violations, drive storage violations, physical access violations, and infrastructure physical protection issues. All sites that use combination locks for physical access should be periodically change the combinations and change the locks when an employee or contractor leaves. The First Financial Associates site had serious findings that had to be addressed immediately.

RECOMMENDATIONS

We recommend that the existing Corporation policy that governs the procedure for protecting and handling of PII be referenced and enforced. Specifically:

-All forms of PII (paper and portable electronic) must be stored in designated file cabinets.

-Cubicle drawers must be locked and keys stored in a secure manner when employees are away from their desks.

-Electronic portable storage devices must be password-protected and their contents must be encrypted using FIPS 140-2 compliant encryption if they are used to store sensitive information.

-Combination locks should be changed periodically.

- Recycling bins used to store PII before it can be properly destroyed must be secured to prevent unauthorized access.

-Field offices must encase or otherwise secure their network equipment in a manner to limit access to only those personnel who must have access.

-The Corporation and SRA must conduct full network vulnerability scans, including field office network and FDCC scans of workstation and laptop computers.

-The Corporation must complete policy and procedure updates to include the procedures and responsibilities of SRA.

-Corporation's policies must be correlated with SRA procedures to show execution of the policy.

-First Financial Associates must be made fully FISMA compliant as soon as possible.

FIELD OFFICE AND HEADQUARTERS SCAN

The original FISMA evaluation statement of work required the Carson's FISMA assessor to travel to each of 10 Corporation field offices to assess their compliance with the Federal Desktop Core Configuration (FDCC) requirements. In order to perform this task, Carson employed the Retina FDCC scanning tool to ascertain the configuration of all laptop and desktop computers at each location.

During the first two site visits it became apparent that the Corporation's network configuration would not permit on-site FDCC compliance scanning. It was agreed that the scans would take place toward the end of the FISMA evaluation and be conducted remotely from the Corporation's headquarters in Washington, D.C. These scans took place, with the cooperation of the Corporation's CISO and SRA, during the first week of October 2010. An inventory of all laptops and desktop computers at each field office was provided by the Corporation. This inventory was validated by the FISMA assessor during a visit to each site and confirmed as being successfully scanned remotely from the Corporation's headquarters.

CONCLUSIONS

Two vulnerable machines were found during FDCC scans run on the headquarters network.

RECOMMENDATIONS

We recommend that all vulnerabilities found be addressed or reviewed by the Corporation and action taken, if warranted. If corrections are made, the machines should be rescanned.

APPENDIX A – DETAILED FINDINGS AND RECOMMENDATION

Findings and Recommendations

Finding # 1: All field site offices that use combination locks for access to the main office or access to computer rooms have never changed the combination, do not change the combination after employee termination, and have no stated policy that governs the procedures for combination locked entryways. Offices using key access do not have accountability for the number of keys distributed to employees.

Recommendation(s)

1. A policy should be created or referenced that governs the procedure for access point mechanisms, including combination locks. It should require that combinations be reviewed and changed periodically, and that changes should be mandatory whenever an employee leaves and or is terminated from a office.
2. Keys and access tools be accounted for and collected in the event of the termination of an employee or contractor.

Finding # 2: The Austin, TX, field offices use Passport portable storage devices to back up and store Microsoft mail exchange inboxes. The external drives are not password protected and the information is not encrypted on the drive. These drives are kept and transported at the employee's discretion.

Recommendation

1. All passport drives and any other external storage devices should be password protected and the data stored on the drives, if sensitive, should be encrypted using a FIPS 140-2 approved encryption algorithm.

Finding # 3: PII was found in unprotected areas of office suites.

- An Atlanta field office intranet portal page, which contained PII, was printed and kept in a cabinet with the key left in the lock.
- In the Austin field office, PII was found on a Passport portable drive in a copy of an e-mail inbox.
- In the New Hampshire office, PII was found in an unsecured recycling bin located on a desk.

Recommendation(s)

1. The Corporation's policy that governs the procedure for protecting PII should be referenced and enforced.
2. All forms of PII (paper and electronic) should be stored in designated lockable file cabinets. All cubicle drawers should be locked and their keys should be stored in a secure manner when employees are away from their desks.

Finding # 4: In the Phoenix, AZ, field office network access was gained by providing an IP address through Dynamic Host Configuration Protocol (DHCP). The laptop was plugged in and given an IP address that allowed the laptop access to the network.

Recommendation(s)

1. All network configurations should be the same for all field offices.
2. Visitors should not be permitted to join the local domain with their laptop computers and obtain an IP address from the local DHCP server.

Finding # 5: Network and telephony equipment, such as switches and patch panels, are openly accessible to everyone working in the field office suites because the equipment is located in common or unsecured office areas. The sole exception is the Richmond office, in which network and telephony equipment is encased and secure from general access.

Recommendation

1. All field offices should encase or secure their network equipment in a manner to limit access to only those personnel who must have access.

Finding # 6: Field office networks are not regularly scanned for vulnerabilities nor are the desktops and laptop computers scanned for compliance with the mandated Federal Desktop Core Configuration.

Recommendation

1. The Corporation and SRA should conduct full network vulnerability scans, including the field office network and FDCC scans of workstation and laptop computers.

Finding # 7: The Corporation's policies are in the process of being updated and are in draft form. A list of the policies in draft was provided, but no evidence of actual draft documents was provided.

Recommendation

1. The Corporation should complete policy and procedure updates, to include the procedures and responsibilities of SRA. Corporation policies must also be correlated with SRA procedures to show execution of the policies.

Finding # 8: Two vulnerable machines were found during FDCC scans run on the headquarters network. Microsoft Windows Default Guest Account is not renamed and disabled, and Microsoft Windows Password Complexity on target system is not configured to enforce password complexity requirements (Machine IP Address [redacted] . Microsoft Windows Anonymous SID/Name could grant an anonymous user a security identifier (SID) (Machine IP Address [redacted]).

Recommendation

1. The default guest account should be renamed and disabled and the password policy setting "Password must meet complexity requirements" should be enabled. Vulnerabilities should be addressed as warranted, based on Corporation policy.

Finding # 9: First Financial Associates' network has no security baseline and does not address any security controls to protect PII, specifically:

1. First Financial Associates' network is vulnerable to attack and is at high risk for compromise.
2. The network does not use password protection to authenticate users on the system, nor are passwords used to log on to the desktop computers.
3. The network and desktops have not employed antivirus protection for the systems.
4. E-mails hold PII and there are no procedures for deletion, maintenance, or protection of the information.

Recommendation(s)

1. First Financial Associates should immediately address the security baseline of the network and hire a professional company to secure its network.
2. First Financial Associates should immediately provide antivirus protection for the server and all workstations conducting Corporation business.
3. First Financial Associates should immediately implement use IDs and passwords to log on to the network and to desktop computers.
4. First Financial Associates should create policies for the deletion and storage of e-mails to protect PII.
5. First Financial Associates should make a decision on a vendor and begin the FISMA compliance process immediately addressing the security controls stated by NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*; Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information Systems*; and FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Finding #10: The Corporation is using MetroFax, which may leave PII exposed within another outside system.

Recommendation

1. First Financial Associates should establish a trust relationship or produce a service-level agreement (SLA) between Metrofax and First Financial Associates to protect any PII information transmitted or stored.

Corporation for
NATIONAL & COMMUNITY SERVICE

November 3, 2010

TO: Kenneth Bach
Acting Inspector General

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

Subject: Corporation comments on OIG Draft FISMA Review Report for Fiscal Year 2010

Thank you for the opportunity to comment on the Draft FISMA review report for Fiscal Year 2010. As noted in the report, the Corporation has taken steps in FY 2010 to continue to improve its information assurance 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 the draft "CNCS FISMA Review for FY 2010" and agrees with the findings and recommendations presented. Indeed, the recommendations are in alignment with CNCS' Strategic Technology Plan and ongoing information assurance projects. In particular, the Corporation has planned the following activities which address the recommendations:

- Continued updating of information assurance documentation to ensure compliance with NIST and OMB privacy and system security guidance.
- Implementation of vulnerability scanning tools to monitor for baseline security compliancy.
- Continuation of efforts to work with information collection owners to review and keep updated the inventory of CNCS Personally Identifiable Information (PII).
- Reduction of unnecessary collection and holding of PII.
- Development of Privacy Impact Assessments (PIAs), System of Record Notices (SORN), and other compliant documentation for systems containing PII.
- Continuation of efforts to work with external system providers to comply with FISMA requirements.

If you have any questions about this response or the planned activities, please contact the Corporation's Chief Information Security Officer at (202) 606-6662.

Cc: James Siegal, Chief of Staff
Robert Velasco II, Chief Operating Officer

Appendix C

INDEPENDENT EVALUATION
FEDERAL INFORMATION SECURITY MANAGEMENT (FISMA)
COMPLIANCE OF
FIRST FINANCIAL ASSOCIATES

BACKGROUND

The Federal Information Security Management Act (FISMA) defines information security as "... protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (i) integrity - guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; (ii) confidentiality - preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (iii) availability - ensuring timely and reliable access to and use of information.

The Office of Management and Budget (OMB) and FISMA has directed that agency contractors or grant recipients who manage federal agency data for or on behalf of a federal agency must follow FISMA guidelines. FISMA, Section 3544(a)(l)(A)(ii), requires that federal agencies perform oversight and evaluation 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, and National Institute of Standards and Technology (NIST) guidelines.

NIST's Federal Information Processing Standards (FIPS) Publication (PUB) 200, Minimum Security Requirements for Federal Information and Information Systems, specifies minimum-security requirements for federal information and information systems in 17 security-related areas. Federal agencies. agency contractors or grant recipients who manage Federal agency data for or on behalf of a Federal agency must meet the minimum security requirements as defined herein through the use of the security controls in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems, as amended.

During FY2010, the Corporation's Chief Information Security Officer (CISO) expressed concerns to the OIG regarding the status of FISMA compliancy of one its contracted vendors, First Financial Associates (FFA) located in Lithonia, Georgia. In FY2010, FFA was selected by the Corporation to manage and administer its Child Care Benefits Program (CCBP) on behalf of AmeriCorps State & National members. FFA is certified as a Small Disadvantaged Business (SDB) by the U.S. Small Business Administration (SBA) and has provided services for a variety of clients, including:

- Federal Government agencies and other public sector agencies including state, county and other local agencies and departments.
- Commercial banks, savings and loan associations, and other types of financial institutions and other financial services companies.
- Public and private corporations.

To determine the status of FFA's FISMA compliance, during August 2010, the OIG's Chief Technology Officer (CTO) and Carson, its independent evaluation contractor, and the Corporation's Chief Information Security Officer conducted a site visit.

OBJECTIVE

The objectives of OIG's FFA's site evaluation were:

- To identify and determine the status of FISMA compliance efforts of FFA.
- To conduct an evaluation of FFA's procedures of protecting personally identifiable information

SCOPE AND METHODOLOGY

The site visit was conducted to evaluate FFA's compliance or efforts to become compliant with FISMA requirements.

OIG's methodology included:

- Conducting interviews with key personnel.
- Inspection of documentation.
- Performance of an information security and PII walkthrough of the FFA facilities.
- Testing of key controls as they relate to information security, PII, and FISMA.

INDEPENDENT EVALUATION

Based on the results of the site visit and evaluation, OIG determined that FAA is not in compliance with FISMA, OMB, or NIST documented requirements. While FFA is currently in the process, with assistance from the Corporation, of procuring the services of a vendor(s) to help it FISMA complaint, its current information security posture places Corporation information in significant peril of compromise.

Findings

1. FFA developed its information system infrastructure without professional advice or development using a life cycle methodology with phases that included information security.
2. FFA's work stations run Windows XP. The administrator is the Chief Executive Officer (CEO), who enlists through a non-contracted means, assistance concerning implementation and maintenance of the system.
3. The logon procedure for the desktops is as follows: Turn on the laptop and boot-up the Windows desktop, with no password required.
4. FFA's Server and work stations have no anti-virus protection and have had limited administrative maintenance.
5. There are no maintenance records for updates and patches. The server has no structured security baseline.

6. FFA uses a third party vendor (MetroFax) to transmit member information directly to FAA analysts via e-mail. This creates an opportunity for PII information to be exposed and/or stored in a system that is outside FFA or the Corporation's control, which may leave PII exposed within another outside system.

CONCLUSION

FFA has serious information security issues that should to be addressed as immediately.

RECOMMENDATIONS

FFA should immediately:

1. Address the security baseline of the network and hire a professional company to secure its network.
2. Provide antivirus protection for the server and all workstations conducting Corporation business.
3. Implement user IDs and passwords to log on to the network and to desktop computers.
4. Create policies for the deletion and storage of e-mails to protect PII.
5. Make a decision on a vendor and begin the FISMA compliance process immediately, addressing the security controls stated by NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations; Federal Information Processing Standards (FIPS) Publication (PUB) 199, Standards for Security Categorization of Federal Information Systems; and FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems.
6. Establish a trust relationship or produce a service level agreement (SLA) with MetroFax to protect any PII that is transmitted or stored.