Office of Inspector General
Corporation for National and Community Service

FEDERAL INFORMATION SYSTEM MANAGEMENT ACT (FISMA) REVIEW FOR FY 2009 CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT NUMBER 10-03

FINAL REPORT

FEBRUARY 5, 2010

Prepared by:

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Inspector General (OIG), Corporation for National and Community Service (Corporation), contracted with Richard S. Carson and Associates (Carson Associates) to perform an independent Fiscal Year (FY) 2009 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

RESULTS IN BRIEF

The Corporation has taken significant steps to enhance its information security program and address issues identified in the 2008 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 revision of system security documentation to comply with NIST recommended guidance.
    - Development and testing of the Corporation Continuity of Operations Plan (COOP) and IT Disaster Recovery Plan.
    - Continued work efforts to improve information privacy and awareness. The Corporation has improved training materials in this area and is in process of validating all systems that contain privacy information. An analysis is currently underway to identify opportunities to reduce the use of Personally Identifiable Information (PII), where applicable.
    - Continued efforts to work with third-party providers identified during prior-year reviews to comply with FISMA requirements.

- System Security Plan templates have been revised, and all Corporation system security plans have been, or are in process of being, updated. This also includes re-evaluating the risk-level categorizations for each of the systems and adjusting the System Security Plans (SSP) accordingly.

- The Corporation continues to work on developing a complete and accurate inventory of all of its systems, both internal and external.

We have made two (2) recommendations in areas needing improvement to further enhance compliance through the Corporation's information security program. The recommendations are summarized on page 12 of this report.

CORPORATION RESPONSE

Carson Associates has reviewed the Corporation's response to the draft report, which is 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
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
CP	Contingency Plan
DISM	Director of Information Security Management
E-SPAN	Electronic-System for Programs, Agreements, and National Service
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FRB Web	Federal Retirement Benefits Calculator
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
IG	Inspector General
IIF	Information in Identifiable Form
IT	Information Technology
LAN	Local Area Network
MA	Major Application
NFC	National Finance Center
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
PBPACS	Personnel Badging and Physical Access Control System
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
ST&E	Security Test and Evaluation

US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture

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*
800-50, *Building an Information Technology Security Awareness and Training Program*
800-53, Revision 1, *Recommended Security Controls for Federal Information Systems*
800-53A (Draft), *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*

February 5, 2010

Kenneth C. Bach, Assistant Inspector General for Support
Corporation for National and Community Service
Office of Inspector General
1201 New York Avenue NW, Suite 830
Washington DC 20525

Reference: Contract Number GS-00F-0001N, Order Number CNSIG09F0001

Subject: Final Fiscal Year 2009 FISMA Independent Evaluation for the Corporation for National and Community, OIG Report Number 10-03

Dear Mr. Bach:

The final FY09 FISMA Independent Evaluation for the Corporation for National and Community Service is provided in compliance with the above contract.

If you have any questions regarding the enclosed document, please contact me at (301) 841-0083 or via e-mail at bradenje@carsoninc.com.

Sincerely,

Signature on File

John E. Braden, Jr.
IT Security Program Manager
Information Technology Services

Enclosures

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 during the period May through September 2009 and covered the following Corporation systems: Corporation Network; Electronic System for Programs, Agreements and National Service (E-SPAN); and Economic Systems Inc. (EconSys) Federal Retirement Benefits Calculator (FRB Web). Our inspection methodology is compliant with the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) is this just CIGIE standards now? "Quality Standards for Inspections," and consists of inquiries, observations, and inspection of Corporation documents and records, as well as direct testing of controls in order to conclude to our objective.

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), NIST, and related authoritative policies, procedures, standards, and guidelines (criteria), where applicable, is 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. Improvements are in process in the following areas:

- System inventory
- System Security Plan
- COOP and contingency planning
- Privacy impact assessments
- Certification and accreditation (C&A) testing and documentation

Recommendations corresponding to these observations are intended to assist the Corporation in determining the action needed to continue the improvement of its information security program and correct identified weaknesses and/or deficiencies.

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 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

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 to perform an annual assessment of its security program.

CONCLUSIONS

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 its 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. Policies are reviewed and revised annually.

SECURITY AWARENESS AND TRAINING

FISMA requires security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities and their responsibilities in complying 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 guidance specified in NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program.*

During 2009, the Corporation's OIT conducted information technology security awareness training for all users and users with significant information technology security responsibilities, including contractors...

SECURITY AND THE SYSTEM DEVELOPMENT LIFE CYCLE (SDLC)

A number of Federal laws and directives require integrating security into the SDLC, including the Federal Information Security Management Act (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 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 was in the process of transitioning to a managed data center. Activities currently underway that require follow-up by agency security personnel include:

- The completion of the Corporation system inventory, which should also include 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 the 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 (GSS).

CONCLUSIONS AND RECOMMENDATIONS

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, Revision 1. We found improvement can be made in the following area:

- The detail of control implementation does not always define the personnel, by name and/or title, responsible for implementation. Corporation templates have been revised to include this detail; however, not all security plans have been updated.

Recommendation:

1) Information System Owners should continue to develop and update the system security plans in accordance with guidance provided by NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems,* using the revised Corporation system security plan template.

CONTINGENCY AND CONTINUITY OF OPERATIONS PLANS (COOP)

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 establish and periodically test an agency's or a department's capability to continue providing service.

CONCLUSIONS

The Corporation has documented its policy for contingency planning. Information owners are responsible for the development of a Contingency Plan or Disaster Recovery Plan for each major information system.

The Corporation has documented its COOP and Disaster Recovery Plan and has documented contingency plans for its network and major applications. However, because the Corporation is in the process of transitioning to a managed data center, these procedures, related agreements, and contingency plans will also need to be revised. Further, the service provider should also test this capability and provide the results of testing.

CONFIGURATION MANAGEMENT (CM)

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

CONCLUSIONS

The Corporation issued security configuration policy through a configuration management plan, configuration management program 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.

The Corporation is currently in the process of moving to a managed data center service. Therefore, configuration management plans/procedures, as well as assigned roles and responsibilities, should be revised. Other documentation the OIG will revisit will include operation and system administration manuals and procedural guides, where applicable.

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 AND RECOMMENDATIONS

The Corporation has a 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.

In a prior year review, it was noted that a PIA had not been completed for all systems. While observations noted during prior year reviews still persist, we found that the Corporation Privacy Program continues to improve. The Corporation is in the process of conducting an inventory and analysis of the use of PII in its information collections, systems, and practices.

Recommendation:

2) Information System Owners, with assistance from the Privacy Officer, should continue the development of PIAs in accordance with OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* and as required by the Corporation's Privacy Policy and C&A procedures.

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 AND RECOMMENDATIONS

The Corporation has established a Risk Management Program composed of several key components recommended in NIST SP 800-30. It has implemented, or is in process of implementing:

- **A Classification Framework** for categorizing information resources. GSS and major applications have been categorized in accordance with FIPS 199. However, not all contractor systems have been characterized.
- **Risk Assessments** to assess the risks and threats to information resources. Risk Assessments are performed as part of the C&A of the GSS and major applications.
- **A Certification and Accreditation** program to periodically assess the effectiveness of the security controls in place for its information systems.
- **Periodic vulnerability testing** to identify system vulnerabilities.

The Corporation has established a policy that requires the performance of C&A and related security controls testing, as well as testing of contingency plans.

We noted that a C&A methodology is in place to evaluate the effectiveness of the security policy and procedures. This methodology is compliant with guidance provided by NIST SP 800-37.

The GSS and major applications have, or are in process of gaining, current C&As and have undergone security control testing during FY 2009.

Table 1. Number of CNCS Systems Certified and Accredited, Security Controls Tested, and Contingency Plans Tested by FIPS 199 Risk Impact Level

FIPS 199 Risk Impact Level	Systems Certified & Accredited	Security Controls Tested in FY 2009	Contingency Plans Tested in FY 2009
High	0	0	0
Moderate	2	2	2
Low	1	0	0
Total	3	2	2

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.

In prior reviews, it was noted that controls in this area appeared to be effective. Because the Corporation is in the process of transitioning to a managed data center, the following areas will require follow-up and revision of procedures by agency personnel, where applicable:

- Service management processes to include Help Desk functions
- Security Operations Center
  - Data collection processes
  - Logging standards and procedures for monitoring collected data
- Incident-handling procedures and compliance with Corporation security requirements

EVALUATION OF AGENCY OVERSIGHT OF CONTRACTOR SYSTEMS

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.”

EconSys is an application service provider that provides a retirement benefits calculator for Federal agencies. This calculator is used by human resource specialists and employees to compute annuity estimates. The application collects personal information, such as Social Security numbers, salary, and other personal information for all employees of all Federal agencies that have purchased this service.

CONCLUSIONS

The Corporation has documented policy and procedures requiring that external systems are compliant with FISMA requirements. The Corporation is to perform oversight and evaluation to ensure information systems used or operated by a contractor of the Corporation, or other organization on behalf of the Corporation, meet the requirements of FISMA, OMB policy, NIST guidelines, and Corporation policy.

In prior years, it was noted that contract wording did not specify the requirement for compliance with the Corporation Security Program Plan. In addition, an effective process was not in place to evaluate contractor security programs for compliance with FISMA. The Corporation has implemented contract wording require compliance with FISMA. It was noted that a formal contract with EconSys was not in place because these services were obtained through the use of a government purchase card. But EconSys is using the FISMA as a guideline in the development of its security plan for FRB Web.

The following observations were noted during the review of EconSys documentation:

1) C&As of external/contractor systems have not been completed, to include preparation of C&A package(s) and testing of system controls as required by NIST SP 800-37.
2) Security plan documentation has been modeled using guidance specified in NIST SP 800-18. However, control implementations are not always adequately described in sufficient detail.
3) EconSys has developed a Contingency Plan for the FRB Web application. Based on inspection, it was noted that the FRB Web Contingency Plan establishes processes to recover the FRB Web application following a disruption, but does not provide direct procedures, based on role, to execute the contingency plan, as recommended by NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*. Contingency test plans and scenarios have not been developed, and the results of testing have not been retained for audit purposes.
4) The Privacy Impact Assessment for the FRB Web does not provide adequate detail of administrative and technological controls in place to secure information stored by the FRB Web.
5) EconSys has contracted for intrusion detection services. However, there is not adequate documentation of the procedures in place for handling incidents.

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.

The POA&M is a Corporation-wide process, incorporating all known information technology security weaknesses associated with information systems used or operated by the Corporation, by a contractor of the Corporation, or other organization on behalf of the Corporation. The POA&M process prioritizes information technology security weaknesses through milestone dates to help ensure significant information technology security weaknesses are addressed in a timely manner and receive appropriate resources. The Corporation maintains a repository for the justification of POA&M closures. Findings and recommendations from all reviews are incorporated into the POA&M, including the results of OIG findings noted in prior reviews.

WAR-WALKING EXERCISE

A vulnerability assessment of the Corporation headquarters was conducted using an assessment technique known as "war-walking." The purpose of this testing is to search for and identify wireless access points to the Corporation and to assess the network security posture/risks in wireless networks that result if/when access points are installed and configured in an insecure manner.

CONCLUSIONS

We attempted to locate unauthorized wireless access points using wireless sniffing tools (e.g., NetStumbler) to capture information regarding access points that are connected to the Corporation's network or are within range of our scanning device. During our scan, we detected unsecured networks; however, we were unsuccessful in locating the wireless access points on Corporation facilities. We concluded that these access points were likely in building(s) adjacent to the Corporation's floors or were owned by tenants in the same building.

CONSOLIDATED LIST OF RECOMMENDATIONS

SECURITY PROGRAM EVALUATION

1) Information system owners should continue to develop and update the system security plans in accordance with guidance provided by NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems,* using the revised Corporation system security plan template.

PRIVACY IMPACT ASSESSMENTS

2) Corporation system owners, with assistance from the Privacy Officer, should continue the development of PIAs in accordance with OMB M-03-22 and as required by the privacy policy and C&A procedures.

MONITORING THE DATA CENTER TRANSITION

The following activities currently under way require agency follow up to ensure that supporting artifacts are adequately documented and remain up to date:

- The completion of the Corporation system inventory that should also include 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, system administration manuals and guides, contingency plans, and configuration management plans, where applicable.

APPENDIX A – ECONSYS FISMA SUMMARY

EXECUTIVE SUMMARY

OMB 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 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 meets 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."

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.

OBJECTIVE

A primary objective of the FISMA program is to ensure the effectiveness of information security controls in Federal agencies. The purpose of our review is to determine if contractor-operated systems are compliant with FISMA requirements. This document highlights the result of our review.

SCOPE AND METHODOLOGY

FRB Web is physically housed in the EconSys corporate offices at 3141 Fairview Park Drive, Suite 700, Falls Church, VA. The current location is in an eight-story building in which EconSys occupies a suite of offices on the seventh floor. A site visit was conducted to perform testing of key controls as relates to FISMA. This included conducting interviews with key personnel, and inspection of documentation.

INDEPENDENT EVALUATION

Based on inspection of documentation provided during this period of review, it was determined that the FRB Web has not been properly Certified and Accredited in accordance with NIST SP 800-37, and is therefore not compliant with FISMA. At the time of review, EconSys management identified that the FRB Web was in process of revision. Therefore, a C&A of the system would be conducted as part of the new version.

Areas for Improvement

1) Certifications and Accreditations of external/contractor systems have not been completed, to include preparation of C&A package(s) and testing of system controls as required by NIST SP 800-37.
2) Security plan documentation has been modeled using guidance specified in NIST Special Publication (SP) 800-18. However, control implementations are not always adequately described in sufficient detail.
3) EconSys has developed a Contingency Plan for the FRB Web application. Based on inspection, it was noted that the FRB-Web Contingency Plan establishes processes to recover the FRB-Web application following a disruption, but does not provide direct procedures, based on role, to execute the contingency plan as recommended by NIST SP 800-34. Contingency test plans and scenarios have not been developed, and the results of testing have not been retained for audit purposes.
4) The Privacy Impact Assessment for the FRB-Web does not provide adequate detail of administrative and technological controls in place to secure information stored by the FRB Web.
5) EconSys has contracted for intrusion detection services. However, there is not adequate documentation of the procedures in place for handling incidents.

Based on discussion with Corporation management, Econsys's services were purchased using a purchase card. A formal agreement was not in place which requires compliance with FISMA and no further action was taken with the vendor since a formal agreement was not in place. As noted during our review, the Corporation has documented policy and procedures requiring that external systems are compliant with FISMA requirements. It is recommended that the Corporation enforce requirements for FISMA compliance through the use of a formal contract or other vehicle.

BACKGROUND

The Federal Information Security Management Act of 2002 (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. Information security programs include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations.

Corporation Policy ISP-S-12-0905 requires that it ensure the security of external systems operated on behalf of the Corporation. This policy applies to external systems that contain Corporation information, or which operate, use, or have access to federal information on behalf of the Corporation. The requirements of this policy are as follows:

1) The Corporation will maintain an inventory of all external systems managed or used on behalf of the Corporation.

2) A Corporation employee will be assigned as the Information Owner for the external system and will be responsible for coordinating with the external system operator to ensure compliance with this policy. This will generally be someone from the business unit that owns the contract or uses the external system.

3) The Corporation will have a signed Memorandum of Understanding (MOU) and Interconnection Security Agreement (ISA) with the operator of each external system that has a direct interconnection with a Corporation-operated system.

   a) These documents will adhere to the requirements specified in NIST Special Publication 800-47.

4) The Corporation will follow NIST guidance, including Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems.

The Corporation has documented procedures (Security Oversight Procedures for Information Services) for the oversight of access to Corporation information. Based on inspection, this documentation provides description of roles and responsibilities, and a high level summary of oversight procedures, but does not provide sufficient details of procedures.

For this period of review, Carson and Associates was tasked with the review of the Federal Retirements Benefits (FRB-Web) application. The FRB Web software is developed and owned by EconSys. The software is licensed to customers for an annual license fee based upon the number and type of users. EconSys has classified the FRB-Web as a Major[1] application with a FIPS 199 Categorization of Moderate.

REVIEW OF ECONSYS SYSTEM SECURITY PLAN

OMB Circular A-130, Management of Federal Information Resources,
Appendix III requires that agencies develop a System Security Plan which must address rules of the system, training, personnel controls, and the agency incident response capability, continuity of support, technical security, and system interconnection.

NIST SP 800-18 requires that all information systems must be covered by a system security plan and labeled as a major application or general support system.

We obtained the FRB Web system security plan and appendices and tested for compliance with NIST SP 800-18. From inspection of the FRB Web Security Plan Appendix C:

1. **Rules of the system** are defined in Appendix C.2 (Section 3.3)
2. **Training** is provided by NIH (**http://irtsectraining.nih.gov/**) (Section 4.8). In addition, the EconSys Employee Handbook requires that all EconSys employees compete basic computer security training. **Note:** Carson Associates requested documentation of training. We were not provided documentation of training for EconSys employees. For regular users of FRB-Web, each agency would be responsible for administering security awareness training to their employees.
3. **Personnel Controls**- [Section 4.1]General personnel policies and procedures for EconSys staff are included in the EconSys Employee Handbook.
4. **Incident Response Capability** are defined in the FRB Web Security Plan Appendix B-EconSys Computer Security Incident Response Plan
5. **Continuity of support** is defined in FRB Web Security Plan Appendix A-FRB Web Contingency Plan
6. **Technical Security**- FRB Web Security Plan Appendix C defines the Management Operational and Technical controls planned or in place for FRB Web. Based on

[1] OMB Circular A-130, Appendix III, defines major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

inspection of the security plan, we noted that controls are not always sufficiently described in the security plan.

7. **System Interconnection**- The FRB Web Security Plan Appendix C section 2.4 defines the System Interconnections which are as follows:
    a. Customers access the FRB-Web via the Internet using a standard browser
    b. Payroll data is downloaded directly from the NFC to the FRB Web network using FTP over a secure remote connection. **Note:** Based on discussion with the Security Manager, the connection does not establish a direct connection between the NFC and EconSys. Instead, a stand-alone machine is used to download a file from NFC. This file is then scanned for viruses, and then uploaded to FRB-Web. A procedure for performing downloads and uploading files have not been formally documented.

We determined that the FRB Web Security Plan does appear to be compliant with requirements defined in NIST SP 800-18. However, supporting documentation of the controls cited in the Security Plan was not available for inspection at the time of our review..

CERTIFICATION AND ACCREDITATION OF FRB-WEB

Security Controls for the FRB Web Application are documented in the FRB Web Security Plan, Appendix C. From inspection, we noted that:

CA-1: The Security Manager is responsible for developing and monitoring EconSys Certification , Accreditation and Security Assessment Policies and Procedures

CA-2: The Security Manager with System and Database Administrators conducts annual review of the FRB Web Security Plan. Section 3.2 requires that the EconSys Security manager conduct an annual review of the security controls defined in the FRB Web Security Plan annually in the month of January, except in the years that an independent review is conducted.

CA-4: The FRB Web Security Plan (pg.33) cites that EconSys has conducted an assessment of the security controls for FRB Web as required by OMB Circular A-130.

CA-5: The FRB Web Security Plan (pg.33) cites that EconSys maintains a plan of action and milestones (POA&M) to track and monitor deficiencies identified in the FRB Web application.

Based on our discussion with the Data Center/ Security Manager, a formal Certification and Accreditation of the FRB-Web system has not been performed. Currently, the FAA is doing itsr own C&A of the FRB-Web. EconSys is also planning on having a third party conduct an independent certification and accreditation for the FRB-Web.

Other reviews have been conducted which include:

- **An audit conducted by the USPS**. The purpose of this review was to evaluate the physical, personnel and information security concerning EconSys continuation of work for the U.S Postal Service (USPS). This site survey determined that EconSys did not meet the USP requirements regarding the protection of sensitive information. The report, dated April 24, 2009, is in draft format. Based on inspection, we determined that the test-work conducted does not appear to include all controls recommended by NIST SP 800-53 for a system with a FIPS 199 categorization of “Moderate”.

- An external scan conducted by OCC resulted in the identification of 54 vulnerabilities in 11 types, and 10 recommendations. Carson Associates noted that the report was not dated. We requested the plan of action and milestone (POA&M) to determine the current status of these issues. We did not receive documentation for review.

Based on review of documentation provided for this period of review, we noted that:

- We are unable to determine if testing if conducted periodically because report dates could not be verified.
- We could not verify the current status of actions to mitigate risks identified as a result of security controls testing because a current POA&M was not provided for review.
- Security controls' testing does not appear to be compliant with guidance specified in NIST SP 800-37, or testing does not appear to be appropriate in scope.

CONTINGENCY AND CONTINUITY PLANNING

FISMA requires agencies to develop, document, and implement an approved agency-wide information security program that includes plans and procedures to ensure the continuity of operations for information systems that support the operations and assets of the agency.

Continuity of support is defined in FRB Web Security Plan Appendix A-FRB Web Contingency Plan.

We inspected the Contingency Plan and supporting documentation and determined that contingency plans and procedures have been documented, but do not adequately detail the procedures for executing the contingency plan. Further, there is not sufficient documentation for testing the minimum processes defined in the FRB-Web Contingency Plan.

PRIVACY IMPACT ASSESSMENTS

Based on inspection of the FRB Web Security Plan Appendix C, FRB Web collects data that is subject to The Privacy Act of 1974 (Social security numbers, salary and other personal information) and, as such, agencies and their employees have the reasonable expectation that prudent measures will be taken to protect this information from any exploitation or disclosure.

FRB Web provides the following notification:

Privacy Act Notice

We are authorized to request PRIVACY ACT information under 5 U.S.C. Chapter 84. Executive Order 9397 authorizes us to ask for your Social Security number, which will be used to identify your account. We will use the information you provide to process the transaction you request on the Web site. This information may also be shared with other Federal agencies to administer your account or for statistical, auditing, or archiving purposes. In addition, we may share the information with law enforcement agencies investigating, prosecuting, or enforcing a violation of civil or criminal law or with other agencies for the purpose of implementing a statute, rule, or order. You are not required by law to provide this information, but if you do not provide it, it may not be possible to process the actions you request on this Web site.

OMB Memorandum M-03-22 provides Guidance for implementing the Privacy Provisions of the E-Government Act of 2002. This guidance applies to all executive branch departments and

agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public.

A Privacy Impact Assessment of the FRB-Web was conducted on August 4, 2009. Carson Associates assessed the FRB-Web PIA using criteria provided in M-03-22, and determined that:

i. FRB-Web collects the following information:
   i. Social Security Number
   ii. Name
   iii. Date of Birth
   iv. Current and historical salary
   v. Retirement coverage code
   vi. Health Insurance enrollment
   vii. Life insurance enrollment and options
   viii. Address

ii. The FRB-Web is a web-based solution that allows employees access to personal and benefits-related information.

iii. Basic employee data is collected in order to produce the retirement estimate. The social security number is not required to compute the estimate, but is used and requested on all forms that are filled out and submitted to OPM. The SSN with the last name is also used to search the database.

iv. Data is accessed by:

   i. Employees, who can access only their own data

   ii. HR Specialists, who can access data for employees for whom they have been granted access

   iii. Administrators, who can access all data for a specific customer

   iv. EconSys Support, which can access all data for all customers

   v. Tech Support, which can access all data for all customers

v. Employee data is provided by the Agency via NFC or other means. Supplemental information not available electronically is entered by the user and is stored in the application database. This data is not shared with other systems outside of FRB-Web.

vi. The FRB-Web PIA does not identify administrative and technological controls in place to secure this information.

vii. The FRB-Web is not the system of record. Records should be maintained

PERSONNEL SCREENING

Corporation policy requires the assignment of a risk designation to all positions and the establishment of screening criteria for individuals filling those positions.

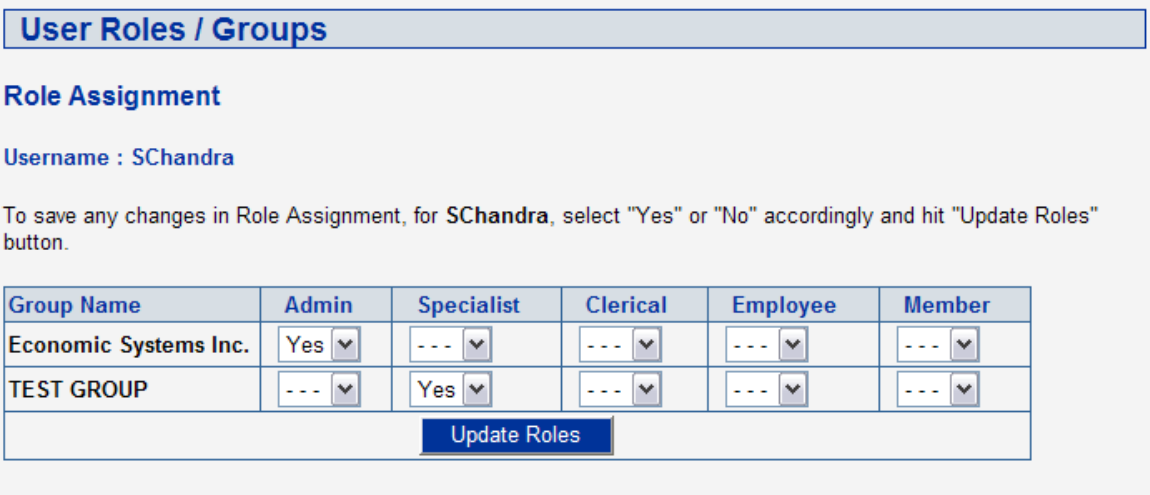
Section 4.1 of the FRB Web Security Plan- Appendix C requires general background screening for both the technical and functional personnel has been accomplished as part of the hiring process, which consists of a careful check of references and former employers. In addition, agency background checks for these staff members are being conducted. All staff working on

the application are required to submit a complete OPM SF85P form (Questionnaire for Public Trust Positions) for background screening. Any staff members that are unable to meet the requirements for security clearance are not allowed to work on the FRB Web or related applications and data.

Appendix C.3 of the FRB Web Security Plan- Appendix C provides detail of EconSys personnel that have access to FRB Web

Name	Role	Clearance Status
Frank Alley	Business Rules Analyst	Cleared
Tom Catalano	Product Manager	Cleared
Robert Taylor	Security Manager	Interim
Haiying Jiao	Technical Support	Cleared
Thiyagarajan Kailasam	Development	Cleared
George Kettner	Corporate Oversight	Cleared
Margaret Rapp	Functional Support	Cleared
Ali Sayer	Operations	Cleared
Martin Rosol	Database Administrator	Cleared

The FRB-web application provides role-based access, as follows:



From discussion with the Security Manager, access is defined by role. Because of the size of EconSys staff, segregation of duties may come into question.

Mitigating processes should be in place as a compensating control and documented in the Security Plan. Procedures should be defined and documentation of review retained for audit purposes. As an example, the FRB-Web system provides audit logs. Based on discussion with the Security Manager, reviews are periodically conducted to ensure that there has been no escalation of privileges. However, there are no formal procedures or automated tools in place for conducting such reviews.

Issues noted:

1. We were unable to validate that Econsys personnel with access to Corporation documentation have been cleared.
2. We were unable to validate that access to Corporation employee data is justified and/or appropriately administered.

INCIDENT HANDLING

Section 4.3 of the FRB Web Security Plan - Appendix C assigns responsibility of handling security issues to the technical support group. This group provides technical support with data issues, defects, browser compatibility, PC settings, Adobe settings and other such issues. This group is also the first point of contact for any security issues, questions or comments.

Incident Response is covered in Appendix B of the FRB Web Security Plan. Carson Associates reviewed this documentation for compliance with NIST SP 800-61. We determined EconSys appears to have a service agreement in place for intrusion detection services. However, we were not provided adequate documentation of procedures in place for detecting, reporting and responding to security incidents.

APPENDIX B – CORPORATION MANAGEMENT RESPONSE

Corporation for
NATIONAL & COMMUNITY SERVICE

January 12, 2010

TO: Kenneth Bach
Acting Inspector General

FROM: Mary Cadagin
Chief Information Officer

Subject: Corporation comments on OIG Draft FISMA Review Report for Fiscal Year 2009

Thank you for the opportunity to comment on the Draft FISMA review report for Fiscal Year 2009. As noted in the report, the Corporation has taken steps in FY 2009 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 2010 to further enhance the program.

Corporation Response
The Corporation has reviewed the draft "CNCS FISMA Review for FY 2009" and agrees with the findings and recommendations presented. Indeed, the recommendations are in alignment with CNCS' new 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 security documentation to ensure compliance with NIST guidance.
- Revision and testing of the COOP and Disaster Recovery plans upon the migration to Managed Data Center Services.
- Completion of an inventory of Personally Identifiable Information (PII) collected and used by the Corporation.
- Reduction of unnecessary collection and holding of PII.
- Development of Privacy Impact Assessments (PIAs) 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) 606-6611.

Cc: Nicola Goren, Chief of Staff