Office of Inspector General
Corporation for National and Community Service

FEDERAL INFORMATION SYSTEM MANAGEMENT ACT (FISMA) REVIEW OF FY 2006 FOR THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT NUMBER 07-09

Corporation for
NATIONAL &
COMMUNITY
SERVICE

Prepared by:

Carson & Associates, Inc.
4720 Montgomery Lane
Bethesda, Maryland 20814

This report was issued to Corporation management on November 1, 2006. The Corporation's response to the draft report noted agreement with the recommendations and is considered to be the Management Decision. Under the laws and regulations governing audit follow up, the Corporation is to complete its corrective actions by November 1, 2007. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

EXECUTIVE SUMMARY

PURPOSE

The objectives of the independent 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 the Fiscal Year (FY) 2005 POA&M.

RESULTS IN BRIEF

The Corporation has taken significant steps to enhance its information security program and address issues identified in the 2005 FISMA report including:

- Appointing an acting Chief Information Officer (CIO) until one entered duty in May 2006
- Documenting several key policies and procedures, including CIO-2006-001: Information Security Program/Policy, dated February 1, 2006
- Documenting a system inventory to include the general support system, major applications, minor applications, and interconnections, both internal and external
- Using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005 (updated June 17, 2005) to complete certification and accreditation (C&A) efforts
- Documenting three management action plan areas, dated June 9. 2006, requiring immediate attention: security, education, training, and awareness (SETA); incident response; and configuration management (CM) plan
- Documenting Privacy Impact Assessments (PIA) for the general support system, major applications, and minor applications
- Documenting e-authentication risk assessments for the general support system, major applications, and minor applications

We have made recommendations in areas needing improvement in order to further enhance compliance through the Corporation's information security program. The Corporation needs to continue building upon its record of accomplishments by implementing corrective actions based on the OIG's recommendations.

CORPORATION RESPONSE

Carson Associates has reviewed the Corporation's response to the draft report. We note that the Corporation is in agreement with all of the findings and recommendations. The findings and resolution will be tracked through the POA&M process. The Corporation's response is included in Attachment A to this report.

ABBREVIATIONS AND ACRONYMS

C&A	Certification and Accreditation
CIO	Chief Information Officer
CM	Configuration Management
CP	Contingency Plan
E-SPAN	Electronic-System for Programs, Agreements, and National Service
FedCIRC	Federal Computer Incident Reporting Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IG	Inspector General
IT	Information Technology
LAN	Local Area Network
MA	Major Application
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PBPACS	Personnel Badging and Physical Access Control System
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SAISSO	Senior Agency Information System Security Officer
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
WBRS	Web-Based Reporting System

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 06-20 – FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

NIST Federal Information Processing Standards (FIPS)

FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems

NIST Special Publications (SP)

800-18 – Guide for Developing Security Plans for Information Technology Systems
800-30 – Risk Management Guide for Information Technology Systems
800-47 – Security Guide for Interconnecting Information Technology Systems
800-53 – 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

TABLE OF CONTENTS

INDEPENDENT EVALUATION

This section provides the conclusions and findings from 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 of Standards and Technology (NIST), and related authoritative policies, procedures, standards, and guidelines (criteria), where applicable, is cited when describing a specific finding (condition).

Recommendations corresponding to these conclusions and findings 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.

The independent evaluation covered the following Corporation systems: CNCS Network, Momentum, Electronic-System for Programs, Agreements and National Service (E-SPAN), Web-Based Reporting System (WBRS) and Personnel Badging and Physical Access Control System (PBPACS).

SECURITY POLICIES AND PROCEDURES

CONCLUSIONS AND FINDINGS

Information security policies and procedures require consistent updating to remain current with changes in law, OMB policy, and NIST standards, and guidance.

Several polices have been documented and revised. Management has many documents in draft or under revision. We encourage management to commit to the finalization of the drafts. OIT documented three action plans (SETA, CM Plan and Incident Response) that have been prioritized, and progress will be reviewed no later than the FY 2007 FISMA Evaluation. Maintaining governance documentation allows the Corporation to protect itself when assessing the accountability of users who access the Corporation's information.

FISMA requires senior agency information security officers (SAISSO) to develop and maintain information security policies, procedures, and control techniques to address all applicable requirements.

We recommend that the Corporation maintain information security policies and procedures to remain current with changes in law, Federal policy, standards, and guidelines, by requiring and conducting defined periodic reviews and updates.

ANNUAL SECURITY REVIEWS

CONCLUSIONS AND FINDINGS

Not all annual security reviews were completed in time for comment in the independent evaluation.

We received annual security review data for the minor applications, but reviews for other systems were not available. FISMA requires each agency to perform, for all systems, "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually." This review shall include the testing of management, operational, and technical controls.

We recommend the Corporation:

- Conduct annual security reviews in a more timely manner by requiring their completion and finalization by June 30 of each year. This will provide time for the inclusion of all required reviews in the FISMA independent evaluation and OMB reporting.
- Use the results of the annual security reviews to update SSPs and RAs. This will assist with the completion of a more efficient C&A effort.

CERTIFICATION AND ACCREDITATION (C&A)

CONCLUSIONS AND FINDINGS

C&A documentation needs enhancement to maintain compliance with NIST-issued guidance.

Management is to be commended for completing C&A packages using NIST SP 800-53 controls. However, additional improvements are needed in all the C&A packages we reviewed. RAs document little evidence of testing controls to ensure they are operating as intended. This should be covered by an ST&E report. A complete ST&E report captures the results for all management, operational, and technical controls. OIT's security testing included automated scanning of its systems and informal reviews of its security practices. This approach does not cover all of the management, operational, and technical controls.

After bringing the ST&E weakness to management's attention, OIT provided spreadsheets that documented limited testing activities. Although control enhancements were documented on these spreadsheets, the degree of implementation was not fully documented to reflect the status of compliance with the security controls. In addition, organization-defined elements required by the NIST SP 800-53 security controls were not consistently documented.

OMB Memorandum 06-20 provides required documentation for C&A activities. C&A requires documentation of security planning. This includes RAs, CPs, incident response plans, security awareness and training plans, information systems rules of behavior, CM plans, security configuration checklists, PIAs, and system interconnection agreements.

NIST SP 800-30 differentiates ST&E from automated vulnerability scanning and penetration testing. The purpose of system security testing is to test the effectiveness of the security controls of a system as they have been applied in an operational environment. In contrast, the potential vulnerabilities identified by automated scanning may not represent real vulnerabilities. Similarly, penetration testing is used to test the system from the viewpoint of a threat-source and to identify potential failures in the information technology system protection schemes.

Compliance with the security control baseline was not completely documented for any of the systems. For example, systems categorized as "Moderate" did not consistently document the required control enhancements. In addition, organization-defined elements were not consistently documented in any of the system security plans, with references to corresponding policies and procedures.

Accreditation decisions were made without testing all contingency plans (CPs) to ensure data were recoverable, if needed. Authorizing officials signed accreditation statements before CP testing activities were completed. We note that CP testing was performed in October 2005 and is scheduled for the last week of September 2006, for the GSS and most MAs. Momentum connectivity was successfully tested in August 2006.

We recommend the Corporation:

- Enhance C&A documentation activities to comply with the latest NIST guidance by thoroughly documenting the status of security control compliance through the performance and documentation of ST&E activities.
- Perform ST&E activities to include the review of management, operational, and technical controls, as prescribed in NIST SP 800-30 and, once finalized, NIST SP 800-53A.
- Perform timely CP testing that will allow authorizing officials to make informed accreditation decisions.

System Security Plans (SSPs)

Conclusions and Findings

SSPs need improvement to comply with guidance issued from NIST.

We commend the Corporation for documenting SSPs; however, management did not consistently record controls from NIST SP 800-53, according to guidance provided in NIST SP 800-18.

NIST SP 800-18, Revision 1, requires the use of NIST SP 800-53 security controls and documenting the security controls in a specific manner. Once the security controls have been selected, tailored, and the common controls identified, each control should be described. This description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what factors have been considered; and 4) an indication if the security control is a common control and who is responsible for its implementation.

During the review of the PBPACS SSP, we noticed management did not apply the Federal Information Processing Standards (FIPS) Publication (PUB) 199 high-water mark principle to document the security categorization based on the type of information associated with the application.

FIPS PUB 199 categorizes security for information systems: For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high-water mark) from among those categories that have been determined for each type of information that is contained in the system.

We recommend the Corporation:

- Update and maintain SSPs to document compliance with each NIST SP 800-53 security control, as prescribed by the latest NIST guidance.
- Provide program offices with guidance on how to apply FIPS PUB 199 and NIST SP 800-60, as they perform their security categorizations to select the initial baselines of NIST SP 800-53 controls.

RISK ASSESSMENTS (RAS)

CONCLUSIONS AND FINDINGS

RAs document little evidence of testing controls to ensure they are operating as intended. This should be covered by an ST&E report that captures management, operational and technical controls.

NIST SP 800-30 states risk management should be conducted and integrated in the system development life cycle (SDLC) for IT systems not merely because it is required by law or regulation, but because it is a sound practice that supports the organization's objectives or mission.

We recommend the Corporation update RA documentation with the results of ST&E activities, to include the review of management, operational and technical controls, as prescribed in NIST SP 800-30 and, once finalized, NIST SP 800-53A.

Security Education, Training, and Awareness (SETA)

Conclusions and Findings

OIT documented a management action plan, dated June 9, 2006, to address SETA and expects SETA to be improved and fully implemented by March 31, 2007.

OIT needs to ensure the incorporation of appropriate guidance from NIST for documented, enforceable compliance.

We recommend the Corporation document system users with significant computer security responsibilities and track their training, consistent with NIST guidance.

Plan of Action and Milestones (POA&M) Process

Conclusions and Findings

OIT captures most known security weaknesses and reports them to OMB quarterly, except for weaknesses found in minor applications.

Weakness found during testing and FISMA findings are incorporated into the POA&M process, and appropriately annotated on the POA&M documents. OIT uses milestone dates to prioritize weaknesses. OIT documented Policy 404 by referencing OMB policy and NIST guidance. The Corporation needs assurance that its minor applications, which are hosted off the CNCS Network, maintain the security of its information and comply with FISMA requirements.

We recommend the Corporation document minor application weaknesses in the POA&M, especially for systems either not supported by the CNCS Network or hosted in locations other than on the CNCS Network.

CONFIGURATION MANAGEMENT (CM)

CONCLUSIONS AND FINDINGS

OIT issued a management action plan, dated June 9, 2006, to address CM at the Corporation. OIT expects CM to be fully implemented by April 30, 2007.

OIT needs to ensure the incorporation of appropriate guidance from NIST for documented, enforceable compliance. OIT needs to fully document its use of minimally acceptable system configuration requirements at the Corporation. OIT uses a hybrid of NIST guidance and Microsoft recommendations to harden the security of its Microsoft operating systems. This has been done because National Security Agency (NSA) guidelines have limited functionality. Manufacturer guidelines and recommendations are being used for the other system platforms at the Corporation – Linux, Oracle, Cisco Router IOS, Symantec Enterprise Firewall, Cisco VPN3030, Apache, and Tuxedo.

We recommend the Corporation incorporate the latest NIST guidance and fully document configuration management plans according to OMB policy.

INCIDENT RESPONSE

CONCLUSIONS AND FINDINGS

OIT issued a management action plan, dated June 9, 2006, to address incident response at the Corporation. OIT expects incident response to be improved and fully implemented by October 31, 2006. OIT needs to ensure the incorporation of appropriate guidance from NIST for documented, enforceable compliance.

We recommend the Corporation incorporate the latest NIST guidance to fully document incident response capabilities.

ASSIGNMENT OF RESPONSIBILITY FOR SECURITY

CONCLUSIONS AND FINDINGS

Users assigned responsibility for security in Corporation systems do not consistently function in that capacity, except for the Momentum application.

Individuals assigned security responsibility in Corporation systems need to be in constant contact with the SAISSO to ensure changes in law, standards, and guidance are consistently applied throughout the Corporation's information security program.

OMB Circular A-130, Appendix III, requires the assignment of security responsibility to individuals who are knowledgeable of the technology used in the system. They must also be knowledgeable of providing security for such technology and of the technical controls that are used.

We recommend the Corporation require individuals assigned with the responsibility for security of their systems to obtain guidance from the SAISSO in all matters pertaining to information security, not limited to C&A activities. Guidance from the SAISSO should include, at a minimum, updates to changes in law, OMB policy, NIST standards, and guidance that affect the systems supporting the Corporation's missions and performing annual security assessments, in addition to the C&A activities.

INTERCONNECTION AGREEMENTS

CONCLUSIONS AND FINDINGS

The Corporation does not consistently document interconnection agreements with vendors identified in system security plans.

OMB Circular A-130, Appendix III, requires obtaining written management authorization, based upon the acceptance of risk to the agency's system, prior to connecting with other systems. Where such connection are authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

NIST SP 800-47 provides additional guidance pertaining to system interconnections. The written authorization should define the rules of behavior and the controls that must be maintained for the system interconnection, and the written authorization should be included in the organization's system security plan.

We recommend the Corporation document interconnection agreements with the organizations that have connections to the CNCS Network, host CNCS applications, and/or operate information systems used by, or on behalf of, the Corporation.

CONSOLIDATED LIST OF RECOMMENDATIONS

Security Policies and Procedures:

1. Maintain information security policies and procedures to remain current with changes in law, Federal policy, standards, and guidelines by requiring and conducting defined periodic reviews and updates.

Annual Security Reviews:

2. Conduct annual security reviews in a more timely manner by requiring their completion and finalization by June 30 of each year. This will provide time for the inclusion of all required reviews in the FISMA independent evaluation and OMB reporting.
3. Use the results of the annual security reviews to update SSPs and RAs. This will assist with the completion of a more efficient C&A effort..

Certification and Accreditation (C&A):

4. Enhance C&A documentation activities to comply with the latest NIST guidance by thoroughly documenting the status of security control compliance through the performance and documentation of ST&E activities.

5. Perform ST&E activities to include the review of management, operational, and technical controls, as prescribed in NIST SP 800-30 and, once finalized, NIST SP 800-53A.

6. Perform timely CP testing that will allow authorizing officials to make informed accreditation decisions.

System Security Plans (SSPs):

7. Update and maintain SSPs to document compliance with each NIST SP 800-53 security control, as prescribed by the latest NIST guidance.

8. Provide program offices with guidance on how to apply FIPS PUB 199 and NIST SP 800-60, as they perform their security categorizations to select the initial baselines of NIST SP 800-53 controls.

Risk Assessments (RAs):

9. Update RA documentation with the results of ST&E activities, to include the review of management, operational and technical controls, as prescribed in NIST SP 800-30 and, once finalized, NIST SP 800-53A.

Security Education, Training, and Awareness (SETA):

10. Document system users with significant computer security responsibilities and track their training, consistent with NIST guidance.

Plan of Action and Milestones (POA&M):

11. Document minor application weaknesses in the POA&M, especially for systems either not supported by the CNCS Network or hosted in locations other than on the CNCS Network.

Configuration Management (CM):

12. Incorporate the latest NIST guidance and fully document configuration management plans according to OMB policy.

Incident Response

13. Incorporate the latest NIST guidance to fully document incident response capabilities.

Assignment of Responsibility for Security:

14. Require individuals assigned with the responsibility for security of their systems to obtain guidance from the SAISSO in all matters pertaining to information security, not limited to C&A activities. Guidance from the SAISSO should include, at a minimum, updates to changes in law, OMB policy, NIST standards, and guidance that affect the systems supporting the Corporation's missions and performing annual security assessments, in addition to the C&A activities.

Interconnection Agreements

15. Document interconnection agreements with the organizations that have connections to the CNCS Network, host CNCS applications, and/or operate information systems used by, or on behalf of, the Corporation.

Appendix A

Corporation for National and Community Service's Response

Corporation for
NATIONAL &
COMMUNITY
SERVICE

October 24, 2006

TO: Robert D. Shadowens
Deputy Inspector General

FROM: David Eisner Elizabeth D. Seale, COO
Chief Executive Officer for David Eisner

Subject: Corporation's response to OIG Draft Report, Fiscal Year 2006 Independent Evaluation of the Corporation for National and Community Service Compliance with the Federal Information Security Management Act.

The Corporation is committed to further enhancing and improving its information security program by implementing the initiatives outlined in the Corporation's response to the OIG Memorandum, dated October 10, 2006, that requests comments on the draft OIG report on the Fiscal Year 2006 Independent Evaluation of the Corporation for National and Community Service Compliance with the Federal Information Security Management Act.

Corporation Response

The Corporation's strategy for improving its information security posture builds on the many noteworthy accomplishments in FY06 and the 15 recommendations in the Inspector General's FY06 report. The Corporation notes that we made great achievements this year as evidenced by the Inspector General current report that listed 11 findings and no reportable deficiencies compared to the FY05 report that had over 30 findings and three significant deficiencies.

The Corporation's assessment of the Inspector General's recommendations grouped them into three major information security improvement areas for FY07. As agreed with the Inspector General, the findings will be initially tracked as weaknesses using the Corporation's Plan of Action & Milestones (POA&M) spreadsheet for the first two FY07 quarters, and then the POA&M will be restructured into a recommendations and improvement format. The Corporation's preliminary assessment of the Inspector General recommendations results in three improvement areas (with supporting recommendations) that are:

- Implement Quality Assurance activities into the information security program by;
    1. Conducting more timely annual security reviews by scheduling their completion in time for the OIG evaluation
    2. Using the results of the annual security reviews to update the System Security Plans and Risk Assessments, which will assist with completing a more efficient C&A effort.
    3. Enhancing Certification and Accreditation documentation activities to comply with the latest NIST guidance by thoroughly documenting the status of security

control compliance through performing and documenting Systems Test and Evaluation (ST&E) activities.

4. Performing ST&E activities to include the review of management, operational, and technical controls as prescribed in NIST Special Publications (SP) 800-30 and, once finalized, NIST SP 800-53A.
5. Performing timely DRP testing to allow authorizing officials to make informed accreditation decisions.
6. Updating Risk Assessment documentation with the results of System Test and Evaluation activities, to include the review of management, operational and technical controls, as prescribed in NIST SP 800-30 and NIST SP 800-53A.
7. Documenting interconnection agreements with the organizations that have connections to the CNCS Network and are hosting CNCS applications.

- Implement the monitoring of information assurance activities to ensure that established processes and procedures are followed by;

8. Updating and maintaining Systems Security Plans (SSPs) to document compliance with each NIST SP 800-53 security control, as prescribed by the latest NIST guidance.
9. Providing program offices guidance on how to apply Federal Information Processing Standard Publication (FIPS PUB) 199 and NIST SP 800-60, as they perform their security categorizations to select the initial baselines of NIST SP 800-53 controls.
10. Documenting minor application weaknesses in the POA&M, especially for systems either not supported by the CNCS Network or hosted in locations other than on the CNCS Network.
11. Requiring individuals assigned with the responsibility for security of their systems to obtain guidance from the SAISSO in all matters pertaining to information security, not limited to C&A activities. Guidance from the SAISSO should include, at a minimum, updates to changes in law, OMB policy, NIST standards, and guidance that affect the systems supporting the Corporation's missions and performing annual security assessments, in addition to the C&A activities.

- Improve the information security program by expanding it so that it;

12. Maintains information security policies and procedures to remain current with changes in law, federal policy, standards, and guidelines by requiring defined periodic reviews and updates to information security program policies and procedures.
13. Incorporates the latest NIST guidance and fully document configuration management plans according to OMB policy.
14. Incorporates the latest NIST guidance to fully document incident response capabilities.
15. Documents users with significant computer security responsibilities and track their training, consistent with NIST guidance.

If you have any questions or wish to discuss the Corporation's response, please contact Rudy Mazariegos, Chief Information Officer, at 202 606-6605.

Cc: Frank Trinity, General Counsel
Nicola Goren, Chief of Staff
Jerry Bridges, Chief Financial Officer
William Anderson, Deputy Chief Financial Officer
Sherry Wright Audit Resolution Coordinator